



**Congressional
Research Service**

Informing the legislative debate since 1914

Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations

Paul W. Parfomak

Specialist in Energy and Infrastructure Policy

June 17, 2014

Congressional Research Service

7-5700

www.crs.gov

R43604

Summary

In the United States, the electric power grid consists of over 200,000 miles of high-voltage transmission lines interspersed with hundreds of large electric power transformers. High voltage (HV) transformer units make up less than 3% of transformers in U.S. power substations, but they carry 60%-70% of the nation's electricity. Because they serve as vital nodes and carry bulk volumes of electricity, HV transformers are critical elements of the nation's electric power grid. HV transformers are also the most vulnerable to intentional damage from malicious acts. Recent security exercises, together with a 2013 physical attack on transformers in Metcalf, CA, have focused congressional interest on the physical security of HV transformers. They have also prompted new grid security initiatives by utilities and federal regulators. Legislative proposals, notably the Grid Reliability and Infrastructure Defense Act (H.R. 4298 and S. 2158), would expand these efforts by strengthening federal authority to secure the U.S. grid.

For more than 10 years, the electric utility industry and government agencies have engaged in a number of initiatives to secure HV transformers from physical attack and to improve recovery in the event of a successful attack. These initiatives include coordination and information sharing, spare equipment programs, security standards, grid security exercises, and other measures. There has been some level of physical security investment and an increasing refinement of voluntary grid security practices across the electric power sector for at least the last 15 years. Several major transmission owners have recently announced significant new initiatives specifically to improve the physical security of critical transformer substations in light of the Metcalf attack.

On March 7, 2014, the Federal Energy Regulatory Commission (FERC) ordered the North American Electric Reliability Corporation (NERC) to submit to the Commission new reliability standards requiring certain transmission owners "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. In its order, FERC states that physical security standards are necessary because "the current Reliability Standards do not specifically require entities to take steps to reasonably protect against physical security attacks." According to FERC's order, the new reliability standards will require grid owners to perform risk assessments to identify their critical facilities, evaluate potential threats and vulnerabilities, and implement security plans to protect against attacks.

There is widespread agreement among state and federal government officials, utilities, and manufacturers that HV transformers in the United States are vulnerable to terrorist attack, and that such an attack potentially could have catastrophic consequences. But the most serious, multi-transformer attacks would require acquiring operational information and a certain level of sophistication on the part of potential attackers. Consequently, despite the technical arguments, without more specific information about potential targets and attacker capabilities, the true vulnerability of the grid to a multi-HV transformer attack remains an open question. Incomplete or ambiguous threat information may lead to inconsistency in physical security among HV transformer owners, inefficient spending of limited security resources at facilities that may not really be under threat, or deployment of security measures against the wrong threat.

As the electric power industry and federal agencies continue their efforts to improve the physical security of critical HV transformer substations, Congress may consider several key issues as part of its oversight of the sector: identifying critical transformers, confidentiality of critical transformer information, adequacy of HV transformer protection, quality of federal threat information, and recovery from HV transformer attacks.

Contents

Introduction.....	1
Congressional Interest	2
HV Transformer Risks and Vulnerability	2
High Voltage Power Transformers.....	2
Manufacture and Cost	4
U.S. Manufacturing Capability	5
HV Transformer Sites in the United States	5
Criticality of HV Transformers.....	6
Physical Vulnerability of HV Transformers	6
Targeting of HV Transformers.....	8
Physical Security Measures for HV Transformers	9
Sector Initiatives for HV Transformer Security.....	10
Coordination and Information Sharing.....	10
DOE’s Energy Sector-Specific Plan.....	11
ESCC’s Critical Infrastructure Strategic Roadmap	12
Transformer Equipment Programs	12
DHS Recovery Transformer Program.....	12
EII Spare Transformer Equipment Program.....	13
NERC Spare Equipment Database	13
Grid Security Exercises and Simulations	14
GridEx and GridEx II.....	14
FERC “Electrically Significant Locations” Study	15
HV Transformer Security Standards.....	16
IEEE Substation Security Standard.....	16
NERC Physical Security Guidance	16
FERC Physical Security Best Practices.....	17
NERC Physical Security Regulations	18
Company-Specific Initiatives	19
The Tennessee Valley Authority.....	19
Pacific Gas and Electric (PG&E).....	20
Dominion.....	20
Bonneville Power Administration	21
Issues for Congress.....	21
Identifying Critical Transformers	21
Confidentiality of Critical Transformer Information.....	22
Adequacy of HV Transformer Protection.....	24
Quality of Federal Threat Information	25
Recovery from HV Transformer Attacks.....	26

Figures

Figure 1. Electric Transmission Network	1
Figure 2. Step-Up and Step-Down HV Transformers in the Grid.....	3
Figure 3. 345 kV Transformer Installation	4

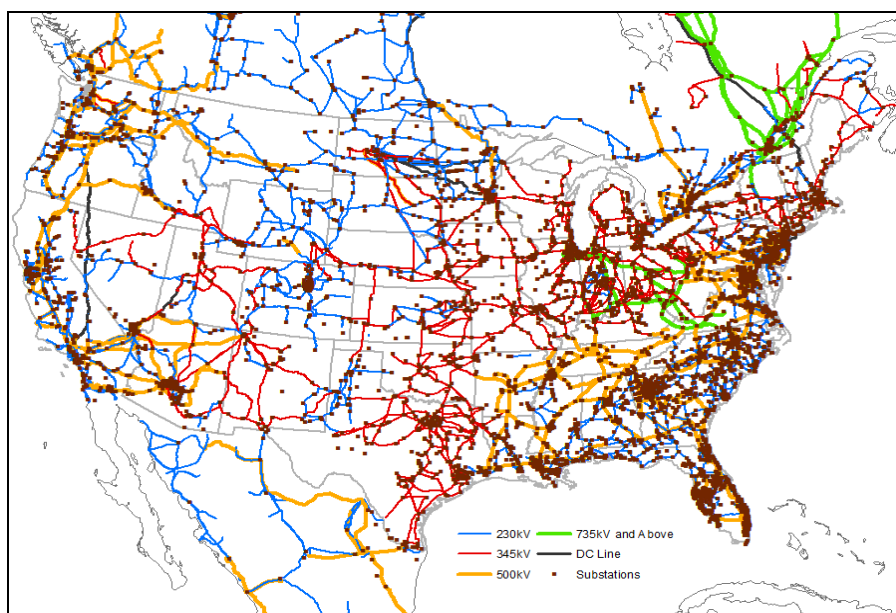
Contacts

Author Contact Information..... 26

Introduction¹

The electric utility industry operates as an integrated system of generation, transmission, and distribution facilities to deliver electric power to consumers. In the United States, this system consists of over 9,000 electric generating units connected to over 200,000 miles of high-voltage transmission lines strung between large towers and rated at 230 kilovolts (kV)² or greater.³ This network is interspersed with hundreds of large electric power transformers whose function is to adjust electric voltage as needed to move power across the network (**Figure 1**). High voltage (HV) transformer units make up less than 3% of transformers in U.S. power substations, but they carry 60%-70% of the nation's electricity.⁴ Because they serve as vital transmission network nodes and carry bulk volumes of electricity, HV transformers are critical elements of the nation's electric power grid.

Figure 1. Electric Transmission Network



Sources: CRS analysis of GIS data from Platts, HSIP Gold 2013 (Ventyx), and Esri.

¹ Portions of this report were drawn from CRS Report R42795, *Electric Utility Infrastructure Vulnerabilities: Transformers, Towers, and Terrorism*, by Amy Abel, Paul W. Parfomak, and Dana A. Shea.

² 1 kV=1,000 volts.

³ North American Electric Reliability Corporation, "Understanding the Grid," fact sheet, August 2013, <http://www.nerc.com/AboutNERC/Documents/Understanding%20the%20Grid%20AUG13.pdf>. Note that there is no industry consensus as to what voltage rating or other operating characteristic constitutes "high voltage." This report uses 230 kV as the high voltage threshold, but other studies may use a different threshold, such as 115/138 kV, or may include an additional "extra high voltage" category above 345 kV. See, for example, U.S. Department of Energy, *Large Power Transformers and the U.S. Electric Grid*, April 2014, p. 4.

⁴ C. Newton, "The Future of Large Power Transformers," *Transmission & Distribution World*, September 1, 1997; William Loomis, "Super-Grid Transformer Defense: Risk of Destruction and Defense Strategies," Presentation to NERC Critical Infrastructure Working Group, Lake Buena Vista, FL, December 10-11, 2001.

The U.S. electric power grid has historically operated with such high reliability that any major disruption, either caused by weather, operational errors, or sabotage, makes news headlines. Such outages can have considerable negative impacts on business, government services, and daily life. Notwithstanding its high reliability overall, the U.S. power grid has periodically experienced major regional outages. Recent examples include the Northeast Blackout of 2003 (which affected 55 million customer in eight states and Canada) and extended outages in the New York/New Jersey area after Superstorm Sandy in 2012.

Congressional Interest

The various parts of the electric power system are all vulnerable to failure due to natural or manmade events. However, for reasons discussed below, HV transformers are considered by many experts to be the most vulnerable to intentional damage from malicious acts. Congress has long been concerned about grid security in general, but recent security exercises, together with a 2013 physical attack on transformers in Metcalf, CA, have focused congressional interest on the physical security of HV transformers, among other specific aspects of the grid.⁵ They have also prompted new grid security initiatives by utilities and federal regulators. Recent legislative proposals, notably the Grid Reliability and Infrastructure Defense Act (H.R. 4298 and S. 2158), would expand these efforts by strengthening federal authority to secure the U.S. grid. The physical security of HV transformers and associated policy issues are the subject of this report.

HV Transformer Risks and Vulnerability

The main risk from a physical attack against the electric power grid—primarily towers and transformers—is a widespread power outage lasting for days or longer. Utilities regularly experience damage to transmission towers due to both weather and malicious activities and are able to recover from this damage fairly rapidly. Thus, while occasionally causing blackouts, physical attacks on towers generally have not resulted in widespread or long-lasting outages. Likewise, the power industry has experienced mechanical failure of individual HV transformers within a single control area resulting in blackouts lasting hours. However, no region in the United States has experienced simultaneous failures of multiple HV transformers. Experts have long asserted that a coordinated and simultaneous attack on multiple HV transformers could have severe implications for reliable electric service over a large geographic area, crippling its electricity network and causing widespread, extended blackouts. Such an event would have serious economic and social consequences. This section discusses in more detail HV transformer characteristics and physical security risks associated with them.

High Voltage Power Transformers

Utility transformers control the voltage of electricity so that it can be synchronized with other power supplies, transmitted long distances, and distributed to customers. Transformers range in size from small, pole-mounted units that may serve a dozen homes to transmission units that serve an entire city. The larger the transformer, the higher the voltage the transformer can handle.

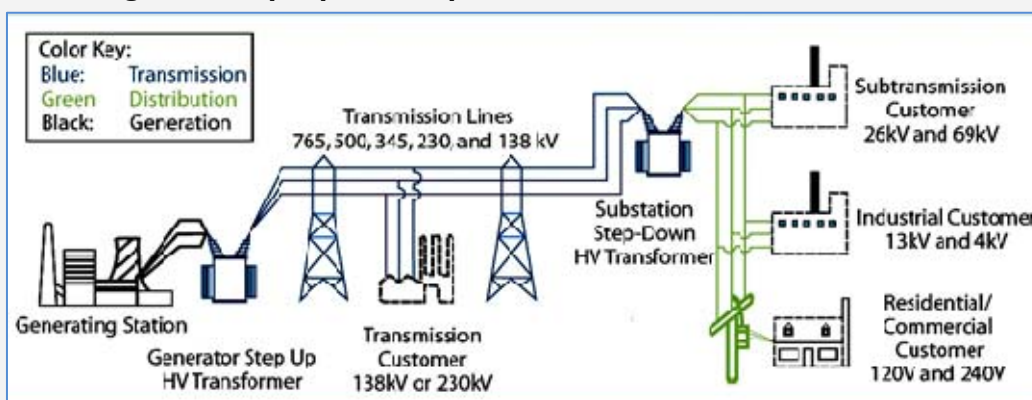
⁵ See, for example: Senators Dianne Feinstein, Al Franken, Ron Wyden, and Harry Reid, letter to the Honorable Cheryl LaFleur, Acting Chairman, Federal Energy Regulatory Commission, February 7, 2014, <http://www.ferc.gov/industries/electric/indus-act/reliability/chairman-letter-incoming.pdf>.

Utility transformers, regardless of size, fundamentally consist of copper wire wrapped around a metallic “core” within an insulated protective housing covered with a 5/8 to 3/4-inch mild steel tank. They are linked to the power grid by protruding metal and (usually) ceramic connectors called “bushings” which resemble giant spark plugs. Larger transformers generate waste heat during operation, so they are cooled by a system of internally circulating oil and external radiators, analogous to the cooling system in a car engine. Transmission transformers are located in network substations along with transmission lines, associated electric equipment, and system controls. These substations may be found in remote locations or near urban centers, depending upon regional transmission needs. Many are located alongside electric generation plants, linking those plants to the grid.

Voltage Management in the U.S. Power System

Electricity produced at U.S. generating stations is converted into a set of three alternating electric currents called three-phase power.⁶ The first step in delivering this power is transforming it from the generated voltage (typically 15-50 kV) to higher voltage (138-765 kV), allowing transmission over long distances in greater volumes most efficiently (**Figure 2**).⁷ This initial voltage step-up occurs by means of transformers located at transmission substations adjacent to the generating facilities. (The three phases of power are carried separately over three wires on transmission towers.) Close to the ultimate consumer, the power is stepped-down at another transformer substation to lower voltages, typically 13 kV or less. At this point, the power is considered to have left transmission and entered the local distribution system.

Figure 2. Step-Up and Step-Down HV Transformers in the Grid



Source: Adapted by CRS from: U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, April 2004, Figure 2.1.

High-voltage transformers, especially units above 345 kV, are physically large and extraordinarily heavy. For example, **Figure 3** shows a new 345 kV transformer many times larger than the pickup truck parked alongside. This transformer unit weighs 435 tons, including 29,000 gallons of cooling oil.⁸ (Note that the vertical bushings are not yet connected to transmission lines because the unit is being moved.) This is a three-phase unit, with one bushing for each of the three phases. Some substations alternatively employ separate single-phase transformers in sets of three.

⁶ The three currents are sine wave functions of time with the same frequency (60 Hertz). The phases are spaced equally, offset 120 degrees from each other. With three-phase power, one of the phases is always nearing a peak.

⁷ The loss of power on the transmission system is proportional to the square of the current (flow of electricity) while the current is inversely proportional to the voltage.

⁸ Pauwels Canada, Inc., personal communication, October 20, 2003.

Generally, the higher the transformer's voltage, the larger the transformer. A three-phase 765kV transformer could be 45 feet tall and occupy a footprint of 2,200 square feet—about the size of an average new single-family house.⁹

Figure 3. 345 kV Transformer Installation



Source: Courtesy of Pauwels Canada, Inc., 2003.

Manufacture and Cost

Most HV transformers are unique and therefore are designed and manufactured to custom specifications for a specific network application. In 2010, the lead time between an HV transformer order and delivery ranged from 5 to 12 months for U.S. manufacturers and 6 to 16 months for foreign manufacturers, although lead times well over 20 months could be required in certain situations.¹⁰ This process may include three to four months for the engineering design alone.¹¹ Since manufacturing generally occurs on a single production line with just-in-time component supplies, advanced production scheduling is important for managing delivery. Physical assembly is labor intensive, requiring manual winding of the copper wire around the transformer core and frequent engineering checks during manufacturing. Extensive testing of completed units also contributes to HV transformer manufacturing time.

The installed cost for an HV transformer depends heavily on its configuration and specific design requirements. New HV transmission substations can cost well in excess of \$10 million, including the cost of transformers and other station equipment. According to the U.S. Department of Energy (DOE), the factory prices for HV transformers typically range from \$2 million for a 230 kV unit to \$7.5 million for a 765 kV unit, before transportation and installation costs.¹²

⁹ U.S. Department of Energy, April 2014, p. 7.

¹⁰ U.S. Department of Energy, April 2014, p. 9.

¹¹ Pauwels Canada, Inc., October 20, 2003.

¹² U.S. Department of Energy, April 2014, p. 7.

U.S. Manufacturing Capability

From 1950 to 1970, utility construction of large generation plants and associated transmission networks fueled a robust U.S. manufacturing market for large transformers. During this period, the United States (and Canada) accounted for approximately 40% of global demand for such units.¹³ After 1970, however, utility investment in transmission infrastructure began falling off due to perceived overcapacity, public resistance to transmission siting, and greater regulatory scrutiny of capital expenditures. Beginning in the late 1980s, uncertainty about industry restructuring and the introduction of competition made grid owners even less willing to invest in new transmission. This decline in U.S. transmission investment greatly reduced domestic demand for large transformers, especially HV transformers. By the late 1990s, the United States and Canada accounted for only 20% of global large transformer sales.¹⁴ Demand in the United States has subsequently increased, however. For example, between 2005 and 2013, the total value of large transformers (including medium- and high-voltage units) imported to the United States more than doubled, from \$284 million (363 units) to \$676 million (496 units).¹⁵

At the same time, global demand for transformers continued to grow and more foreign manufacturers entered the market. According to U.S. industry representatives, many of these foreign manufacturers benefited from dramatically lower labor costs, so they could underbid U.S. transformer makers for the remaining U.S. demand. Some of these foreign manufacturers may have been protected by import barriers which effectively closed their home markets to U.S. transformer imports. Today, there is limited manufacturing capacity in the United States for HV transformers. Five U.S. facilities state that they can manufacture transformers rated 345 kV or above, although it is not clear how many units in this range they have actually produced. Canada and Mexico have five additional HV manufacturing plants.¹⁶ While limited domestic HV transformer manufacturing may increase delivery time, utilities have not reported difficulty in obtaining needed equipment.

HV Transformer Sites in the United States

There are several thousand HV transformers operating in the United States. Approximately 2,100 are very large units rated 345 kV and above.¹⁷ Investor-owned utilities own most of these, although public utilities such as the Power Marketing Administrations (i.e., Bonneville Power Administration and Western Area Power Administration), Tennessee Valley Authority, and the Los Angeles Department of Water and Power own many HV transformers as well.¹⁸ HV transformer substations are distributed throughout the electric grid, as shown in **Figure 1**, with the greatest number in the eastern part of the country.

¹³ C. Newton, "The Future of Large Power Transformers," *Transmission & Distribution World*, September 1, 1997.

¹⁴ C. Newton, September 1, 1997.

¹⁵ U.S. Department of Energy, April 2014, p. 27.

¹⁶ Kenneth Friedman, U.S. Department of Energy, "DOE Update on GMD/EMP-Related Activities," Presentation to the Geomagnetic Disturbance Task Force Working Group, North American Electric Reliability Corporation, November 13, 2013.

¹⁷ John Kappenman, *Geomagnetic Storms and Their Impacts on the U.S. Power Grid*, Meta-R-319, Metatech Corp., prepared for Oak Ridge National Laboratory, January 2010, p. 1-14, http://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc_meta-r-319.pdf.

¹⁸ HV substation information for specific investor-owned utilities is publicly available in annual reports filed with the Federal Energy Regulatory Commission (FERC Form-1).

Criticality of HV Transformers

Because they carry so much electricity, the destruction of HV transformers can seriously reduce the transmission capacity of a regional electric power grid and lead to extended blackouts. The impact of such a failure would depend on the electricity flows in that part of the grid, congestion from major network bottlenecks, and the status of other key facilities such as power plants, transmission lines, and other substations. Power grid planners generally anticipate the possible loss of a single HV transformer substation and are prepared to reroute power flows as necessary to maintain regional electric service. But the simultaneous loss of multiple HV transformers, especially in a constrained transmission area, could exceed the capability of a regional network to reroute power through secondary lines.¹⁹

Numerous publicly available studies have analyzed the risks of a multiple HV transformer failure. For example, the Congressional Office of Technology Assessment (OTA) in a 1990 report on the physical vulnerability of the electric power system found that

In most cases, the nearly simultaneous destruction of two or three transmission substations would cause a serious blackout of a region or utility, although of short duration where there is an approximate balance of load and supply.... The destruction of more than three transmission substations would cause long-term blackouts in many areas of the country.²⁰

In such an emergency scenario, limited electric service could likely be restored in the short term by imposing “rolling” blackouts, rerouting transmission, and using portable transformers. Nonetheless, the loss of key HV substations would leave the regional network crippled and highly susceptible to further disturbance and cascading failure.²¹ According to power industry experts, certain parts of the U.S. transmission network are particularly vulnerable to HV substation disruption. These areas may have severely constrained transmission paths relying on a small number of HV transformers in extremely critical network locations. According to press accounts, a FERC power flow analysis in 2013 identified 30 such critical HV transformer substations across the continental United States; disabling as few as nine of these substations during a time of peak electricity demand reportedly could cause a “coast-to-coast blackout.”²² Not all industry experts agree on the potential severity and duration of a blackout from a multi-transformer attack, however, although it is generally accepted that severe outages may be technically possible.²³

Physical Vulnerability of HV Transformers

All HV transformers are designed to withstand operational risks such as lightning strikes, hurricanes, and network power fluctuations—but they are vulnerable to intentional physical attacks. Despite their great size and internal complexity, HV transformers can be readily disabled or destroyed. According to one manufacturer, “if someone were to intentionally try ... it is a

¹⁹ National Research Council (NRC), *Terrorism and the Electric Power Delivery System*, 2012, p. 69.

²⁰ Office of Technology Assessment (OTA), *Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage*, OTA-E-453, June 1990, p. 37.

²¹ See, for example, Réka Albert, István Albert, and Gary L. Nakarado, “Structural Vulnerability of the North American Power Grid,” *Physical Review E*, Vol. 69, 025103(R), 2004.

²² Rebecca Smith, “U.S. Risks National Blackout From Small-Scale Attack,” *Wall Street Journal*, March 12, 2014.

²³ Rebecca Smith, “Assault on California Power Station Raises Alarm on Potential for Terrorism,” *Wall Street Journal*, February 5, 2014.

surprisingly simple task and there are a large number of ways to conceivably damage a transformer beyond repair.”²⁴ Transformer experts have asserted that a bad actor with basic knowledge of transformer design could inflict irreparable damage. Such attacks can cause massive electrical short circuits and oil fires that would destroy an HV transformer and damage surrounding infrastructure. One fire at a 345 kV substation in Texas, for example, destroyed the transformer and burned for five hours, causing “plumes of smoke that could be seen for miles.”²⁵ In addition to direct attacks on the transformers themselves, HV substations can be further disabled by damaging associated transmission lines or control centers that may be located on site.

Because HV transformers are so big and are connected to the largest overhead transmission towers, they are easily identified along major transmission corridors. High voltage transformers are usually housed in substations that are enclosed with a chain-link fence. Guards are not often stationed at these facilities under normal operating circumstances. Consequently, HV transformers are ordinarily easier to access than other critical electric facilities such as generation plants and control centers. Utilities use closed-circuit surveillance and other methods to detect intrusion. However, access to the substation may be achieved by either cutting or scaling the chain-link fence. Once inside, a saboteur could cause damage by accessing the control room or physically damaging the HV transformer. Penetrating the 5/8 to 3/4-inch steel tank with any device could short-circuit the windings and irreparably destroy the transformer. Alternatively, a saboteur could attempt to open a valve and drain the insulating oil. Igniting the oil might cause the transformer to arc and eventually explode. With a clear line of sight, an attacker could also disable transformers from a distance using conventional rifles.

The vulnerability of individual transformer substations has been demonstrated by successful attacks in recent years. In the most serious case, a rifle attack occurred in April 2013 at PG&E’s 500 kV substation in Metcalf, CA. In this attack, multiple individuals outside the substation reportedly shot at the HV transformer radiators with .30 caliber rounds, causing them to leak cooling oil, overheat, and become inoperative.²⁶ In October 2013, the U.S. Justice Department charged an individual with attacks on the transmission grid in Arkansas, including a deliberate fire at Entergy’s 500 kV substation in Lonoke County. The fire consumed the substation control house but electrical service was not interrupted.²⁷ In 2005, at a Progress Energy substation in Florida, a rifle attack ruptured a transformer oil tank, ultimately causing an explosion and local blackout.²⁸ Other attacks on substation equipment have been reported with some regularity, although most have been attributed to vandals or careless hunters.

It is very difficult to restore a damaged HV transformer substation. As noted above, transmission experts assert that most HV transformers currently in service are custom designed and, therefore, cannot be generally interchanged. Furthermore, at \$3-5 million per unit or more, maintaining large inventories of spare HV transformers solely as emergency replacements is prohibitively costly, so limited extras are on hand. The number of spares a utility maintains is increasingly sensitive information, but one regional transmission control area reported in 2007 that it

²⁴ Mitsubishi Electric Power Products, Inc., personal communication, Warrendale, PA, September 23, 2003.

²⁵ Lower Colorado River Authority, “August 6 Update on Transformer Fire,” press release, Austin, TX, August 6, 2003.

²⁶ RTO Insider, “Substation Saboteurs ‘No Amateurs’,” April 2, 2014, <http://www.rtoinsider.com/pjm-grid2020-1113-03/>.

²⁷ Chelsea J. Carter, “Arkansas Man Charged in Connection with Power Grid Sabotage,” CNN, October 12, 2013; Max Brantley, “FBI Reports Three Attacks on Power Grid in Lonoke County,” *Arkansas Times*, October 7, 2013.

²⁸ Jim Peppard, “Reward Offered in Power Transformer Shooting,” WTSP News (Tampa), October 17, 2005.

maintained 29 spares for 188 transformers rated 500 kV on its system.²⁹ Programs for the sharing of spare HV transformers among multiple utilities are discussed later in this report.

Within the United States, transportation of HV transformers is difficult. Due to their size and weight, most HV transformers are transported on special railcars, each with up to 36 axles to distribute the load. There are fewer than 20 of these railcars in the United States rated to carry 500 tons or more, which can present a logistical problem if they are needed in a transformer emergency.³⁰ Some specialized flatbed trucks can also carry heavy transformer loads over public roadways, but the few such trucks that exist have less carrying capacity and greater route restrictions than the railcars because HV transformers may exceed highway weight limits.

Targeting of HV Transformers

Malicious individuals could, without significant training, identify critical HV transformer locations and time an attack for greatest effect. This could be accomplished with basic knowledge of transmission operations and regional network characteristics drawn from publicly available sources, including electric marketing data indicating constrained areas of the network.³¹ As stated in a 2012 National Research Council report, “terrorists could selectively target key equipment, especially large transformers.”³² The OTA report describes such a scenario:

[One] example is a city served by eight transmission substations spread along a 250-mile line and located in five States. A knowledgeable saboteur would be needed to identify and find the eight transmission substations. A highly organized attack would also be required. However the damage would be enormous, blacking out a four-State region, with severe degradation of both reliability and economy for months.³³

In 1997, the Irish Republican Army reportedly planned this kind of coordinated attack against six transmission substations in the United Kingdom. Although the attack was prevented, had it been successful it reportedly could have caused widespread power outages in London and the South East of England for months.³⁴

It is relatively easy to learn about HV transformer vulnerabilities from engineers and operators experienced with this technology, either domestically or abroad, since the same technology is used in power grids throughout the world. In the past, transformer experts have provided CRS with detailed descriptions of numerous “simple” ways terrorists could destroy HV transformers. General transformer sabotage information is also available on the Internet. One sabotage manual associated with white supremacist groups available online includes the following discussion:

²⁹ David Egan and Kenneth Seiler, PJM Interconnection, “PJM Manages Aging Transformer Fleet,” *T&D World*, March 1, 2007.

³⁰ Tom Daspit, “Schnabel Cars in Service,” web page, August 15, 2013, http://southern.railfan.net/schnabel/schnabel_cars.html.

³¹ Marija Ilic, Professor, Engineering and Public Policy and Electrical and Computer Engineering, Carnegie Mellon Univ., Pittsburgh, PA, personal communication, September 22, 2003.

³² NRC, 2012, p.79.

³³ OTA, June 1990, pg. 37.

³⁴ Stewart Tendler, “IRA Bombers Plotted to Black Out London and South East for Months,” *The Times*, London, England, April 12, 1997.

The power generation and distribution systems of most major Western cities are surprisingly vulnerable.... Attacking during peak consumption times (Winter in cold climates and Summer in hot climates) will make power diversion impossible.... Arson, explosives or long-range rifle fire can be used to disable substations, transformers and suspension pylons. A simultaneous attack against a number of these targets can shut down power ... with the advantage that service cannot be quickly restored by diverting power from another source. Each broken link in the power grid must be repaired in order to fully restore service. An individual, equipped with a silenced rifle or pistol, could easily destroy dozens of power transformers in a very short period of time.³⁵

Security analysts and other industry officials acknowledge that the vulnerability of HV transformers in general is widely known, although understanding the criticality of particular assets within the power grid would require more dedicated effort.

Physical Security Measures for HV Transformers

Although HV transformers are relatively large and often exposed, frequently in rural areas, there are a number of measures available to help prevent an intentional physical attack against a transformer substation. Many of these measures are employed for public safety and to protect against theft, so they may serve multiple purposes. Although security measures appropriate for a particular substation vary depending upon its particular configuration and operating profile, such measures fall into a set of general categories:

- **Protecting information** about critical HV substations, such as engineering drawings, power flow modeling runs, and site security information, which could be useful to a potential attacker.
- **Surveillance and monitoring** through the use of video cameras, motion detectors, imaging, acoustical monitors, aerial drones, and periodic inspection by security employees.
- **Restricting physical access**, such as limiting entry only to necessary employees, installing electronic locks and other access controls, and erecting physical barriers and controls for vehicle entry. Posting full-time guards may also be an option in some circumstances.
- **Shielding assets** from offsite attacks using visual barriers such as opaque or hardened fencing, erecting taller fences, or erecting protective walls.
- **Modifying substation designs** to make them more resistant to physical damage, for example, by strengthening transformer cooling systems or bushings. Reconfiguring substation layouts to limit asset visibility or limit the spread of fire may also be options.

Industry and federal efforts to promote the deployment of such physical security measures are discussed later in this report. In addition to these categories, other measures can help to mitigate the immediate effects of a successful attack (“resiliency”), or to speed full system recovery from such an attack. Measures to enhance the cybersecurity of substation information and control

³⁵ Axl Hess (a.k.a. Aquilifer), *White Resistance Manual V2.4*, 2001. See also Herschel Smith, “A Terrorist Attack That America Cannot Absorb,” *captainsjournal.com*, blog, September 28, 2010, <http://www.captainsjournal.com/2010/09/28/a-terrorist-attack-that-america-cannot-absorb/>.

systems, especially supervisory control and data acquisition (SCADA) systems are an important component of power grid security and are usually coordinated with physical security measures.

Sector Initiatives for HV Transformer Security

Over the last decade or so the electric utility industry and government agencies have engaged in a number of initiatives to secure HV transformers from physical attack and to improve recovery in the event of a successful attack. These initiatives include coordination and information sharing, spare equipment programs, security standards, grid security exercises, and other measures discussed below.

Coordination and Information Sharing

The *National Infrastructure Protection Plan* (NIPP), initially published by the Department of Homeland Security in 2006, “outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes.”³⁶ The plan organizes critical infrastructure into distinct sectors, designating a federal department or agency as the lead coordinator for each sector—the Sector Specific Agency (SSA). Under the NIPP and Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience, the Department of Energy (DOE) is designated as the SSA for the Energy Sector, which includes the electric utility industry (excluding nuclear power plants). As an SSA, the department is responsible for working with the Department of Homeland Security (DHS), other federal agencies, critical infrastructure owners, independent regulators, and other agencies to implement national policy on critical infrastructure security and resilience.³⁷ The NIPP also establishes a sector partnership model including private and government coordinating councils:

- The **Electricity Subsector Coordinating Council (ESCC)**, initially established in 2004, was organized and administered by companies in the electric power industry to meet regularly to coordinate policy-related activities designed to “improve the reliability and resilience of the electricity subsector, including physical and cyber infrastructure.”³⁸ Through August 15, 2013, the ESCC was chaired by the North American Electric Reliability Corporation (NERC), the not-for-profit organization responsible for ensuring the reliability of the North American grid.³⁹ The ESCC has since transitioned to a new structure led by electric utility industry executives, although NERC’s chief executive officer remains on the ESCC steering committee.⁴⁰

³⁶ Department of Homeland Security (DHS), “National Infrastructure Protection Plan,” web page, April 7, 2014, <https://www.dhs.gov/national-infrastructure-protection-plan>. The NIPP was mandated under Homeland Security Presidential Directive 7 issued on December 17, 2003.

³⁷ Presidential Policy Directive 21, *Presidential Policy Directive—Critical Infrastructure Security and Resilience*, February 12, 2013.

³⁸ North American Electric Reliability Corporation (NERC), “Electricity Sub-sector Coordinating Council,” web page, April 7, 2014, <http://www.nerc.com/pa/CI/Pages/ESCC.aspx>.

³⁹ Among other functions, NERC develops and enforces reliability standards, monitors the grid, and trains industry personnel. In the United States, NERC is subject to FERC oversight.

⁴⁰ Gerry W. Cauley, North American Electric Reliability Corporation (NERC), letter to U.S. Secretary of Energy Ernest (continued...)

- The **Energy Sector Government Coordinating Council (EGCC)**, also established in 2004, is the government counterpart to the ESCC. The EGCC is chaired by the DOE and DHS, incorporating other agencies at all levels of government with interest in energy security. The EGCC plays a key role in implementing the Sector-Specific Plan (discussed below), collaborating with the ESCC to develop and prioritize security programs and initiatives.⁴¹

In addition to these councils, other organizations have been established with more specific responsibilities related to grid security.

- The **Electricity Sector Information Sharing and Analysis Center (ES-ISAC)**, established in 1998, is the electricity sector's primary communications channel for security-related information, situational awareness, incident management, and coordination.⁴² The ES-ISAC is operated by NERC in collaboration with the DOE and ESCC. Members may anonymously share security-related incident information with the ES-ISAC 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.⁴³
- NERC's **Critical Infrastructure Protection Committee (CIPC)** coordinates NERC's security initiatives and advises NERC's Board of Trustees, its standing physical and cybersecurity committees, and the ES-ISAC. One of the CIPC's key functions is developing, reviewing, and revising security guidelines; and assisting in the development and implementation of NERC standards.⁴⁴

DOE's Energy Sector-Specific Plan

The 2006 *National Infrastructure Protection Plan* required each critical infrastructure sector to develop a Sector-Specific Plan (SSP) that describes strategies to protect its critical infrastructure, outlines a coordinated approach to strengthen its security efforts, and determines appropriate funding for these activities. The section of the DOE's *Energy Sector-Specific Plan* addressing electricity was developed in collaboration with the ESCC and EGCC. The plan identifies high-voltage transformers as an electric sector vulnerability due to their criticality to the power grid and the difficulty of replacing them in the event of a successful attack. Among other measures, the SSP established a goal of implementing "agreements that require participants to maintain transformers for possible sharing in the event of a terrorist act."⁴⁵ The plan also identified the "need for a new type of emergency spare (recovery/mobile) high-voltage transformer that can be

(...continued)

Moniz, August 23, 2013, <http://www.publicpower.org/files/PDFs/DOESecLetterHistoryESCC.pdf>.

⁴¹ Department of Energy, *Energy Sector-Specific Plan*, 2010, p. 20.

⁴² The ES-ISAC was established under Presidential Decision Directive 63, May 22, 1998.

⁴³ Electricity Sector Information Sharing and Analysis Center (ES-ISAC), "Frequently Asked Questions," web page, <https://www.esisac.com/SitePages/FAQ.aspx>.

⁴⁴ North American Electric Reliability Corporation (NERC), "Critical Infrastructure Protection Committee (CIPC)," web page, <http://www.nerc.com/comm/CIPC/Pages/default.aspx>, April 8, 2014.

⁴⁵ Department of Homeland Security, *Energy Sector-Specific Plan*, 2010, p. 54.

deployed and energized quickly to rapidly recover from outages caused by natural disasters and deliberate attacks.”⁴⁶

ESCC’s Critical Infrastructure Strategic Roadmap

In November 2010, the Electricity Subsector Coordinating Council published its *Critical Infrastructure Strategic Roadmap* report, to provide a framework for identifying risks that could seriously disrupt the grid and for promoting actions to enhance grid reliability and resilience. The report paid particular attention to “severe-impact risks with the potential to impact large portions of the grid, or disrupt service for an extended period of time.”⁴⁷ The report considered three principal risk scenarios, including

Scenario 1: Physical Attack on Significant Electricity System Equipment

A coordinated physical attack on key nodes of the bulk power system critically disables difficult to replace equipment in multiple generating stations or substations and could have a significant affect [sic] on the remainder of the system. A prolonged period of time is required to fully restore the bulk power system to normal operation.⁴⁸

The report recommended a current capability assessment to prevent and respond to such a scenario as a “high priority.” The report also recommended as “important” both a study of “options and practices to enhance physical protection of critical equipment requiring long recovery times (e.g., large high-voltage transformers)” and an initiative to “enhance the availability of critical spare equipment ... starting with high voltage transformers.”⁴⁹

Transformer Equipment Programs

Consistent with the recommendations of the studies above, several programs have been instituted within the electric power sector to address the operational issues that emerge due to the scarcity of spare HV transformers and associated equipment in the event of a physical attack or other grid emergency.

DHS Recovery Transformer Program

In 2008, the Department of Homeland Security (DHS) initiated a program to develop a prototype “Recovery Transformer” (RecX) which could enable recovery from transformer failure within days rather than months or longer.⁵⁰ The RecX transformer was intended to be adaptable to a range of common grid specifications as well as being smaller, lighter, easier to transport, and quicker to install than conventional HV transformers. The RecX prototype was designed to replace the most common HV transformers (345 kV) used in the U.S. grid.⁵¹ This configuration

⁴⁶ Department of Homeland Security, *Energy Sector-Specific Plan*, 2010, p. 70.

⁴⁷ North American Electric Reliability Corporation (NERC), *Critical Infrastructure Strategic Roadmap*, November 2010, p. 2, http://ccpic.mai.gov.ro/docs/NERC_ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf.

⁴⁸ NERC, November 2010, p.18. This scenario involved the loss of three HV substations serving large urban centers with a restoration time to 100% operating capacity of 6-18 months.

⁴⁹ NERC, November 2010, pp.19-20.

⁵⁰ The program was partly funded by the DHS Science and Technology Directorate in a consortium with the Electric Power Research Institute, CenterPoint Energy, and ABB.

⁵¹ ABB, “US Rapid Recovery Transformer Initiative Succeeds Using Specially-Designed ABB Transformers,” press (continued...)

reportedly could be used to replace approximately one quarter of the 2,100 transformers in this voltage class currently deployed.⁵² In 2012, the only three single-phase RecX prototype units were installed in an operating 345 kV substation in Texas during a simulated emergency drill. The units remain in operation, having met or exceeded their service requirements. Although the RecX transformers have reliability and efficiency characteristics comparable to other 345 kV transformers, and are also comparably priced (\$7.5 million each), the manufacturer had received no orders for commercial production of these units as of February 2014.⁵³ Having successfully demonstrated the RecX concept, the DHS is no longer funding the RecX program.

EEI Spare Transformer Equipment Program

In 2006, Edison Electric Institute (EEI), the main trade association for U.S. investor-owned electric utilities, initiated its Spare Transformer Equipment Program (STEP) to strengthen “the sector’s ability to restore the nation’s transmission system more quickly in the event of a terrorist attack.”⁵⁴ The STEP program requires participating utilities to maintain (or acquire) a specific number of transformers up to 500 kV to be made available to other utilities in case of a critical substation failure. Sharing of transformers is mandatory based on a binding contract subject to a “triggering event”—a coordinated act of deliberate, documented terrorism resulting in the destruction or disabling of a transmission substation and the declaration of a state of emergency by the President.⁵⁵ FERC granted blanket authorization for the transfer and cost recovery of transmission equipment under the STEP program in September 2006.⁵⁶ State regulators with jurisdiction over participating utilities have also granted pre-approval for STEP transfers.⁵⁷ The program is designed to deal with terrorist events, but it also provides a mechanism for voluntary sharing of transformers in other emergencies, although these may require additional regulatory approvals. EEI requires annual recertification and conducts a STEP program drill every summer to ensure the program and its members will be fully prepared to respond in the event of an actual triggering event.⁵⁸

NERC Spare Equipment Database

In 2012, NERC initiated its Spare Equipment Database (SED) program intended to serve as a tool to “facilitate timely communications between those needing long-lead time equipment damaged

(...continued)

release, October 4, 2012.

⁵² Matthew L. Wald, “A Drill to Replace Crucial Transformers (Not the Hollywood Kind),” *New York Times*, March 14, 2012.

⁵³ National Research Council (NRC), *The Resilience of the Electric Power Delivery System in Response to Terrorism and Natural Disasters: Summary of a Workshop*, 2013; Sarah Mahmood, Department of Homeland Security, personal communication, February 10, 2014.

⁵⁴ Edison Electric Institute (EEI), “Spare Transformers,” web page, April 10, 2014, <http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx>.

⁵⁵ Edison Electric Institute (EEI), “Overview of the Spare Transformer Equipment Program,” slide presentation, February 23, 2014.

⁵⁶ Federal Energy Regulatory Commission, *Order on Application for Blanket Authorization for Transfers of Jurisdictional Facilities and Petition for Declaratory Order*, Docket Nos. EC06-14-000 and EL06-86-000, September 22, 2006.

⁵⁷ EEI, February 23, 2014.

⁵⁸ Edison Electric Institute, briefing for the Congressional Research Service, February 23, 2014.

in a [High Impact, Low Frequency] event and those equipment owners who may be able to share existing equipment being held as spares by their organization.”⁵⁹ The SED program is a confidential web-based catalog of spare transformers rated at 100 kV or higher. Only NERC and the equipment owners can see their spares data (although NERC can make high-level reports to FERC); requests for equipment are double-blind. Participation is voluntary and requires no commitment or mandatory sharing of spares.⁶⁰ Unlike EEI’s STEP program, however, the SED program has not been granted pre-approval from FERC or state regulators for equipment transfers. Thus, the ability to transfer the ownership of transformers from one company to another may require additional approvals, even during an emergency.

Grid Security Exercises and Simulations

NERC and FERC have conducted grid security computer simulations and exercises specifically incorporating hypothetical attacks on HV transformer substations.

GridEx and GridEx II

In 2011, NERC conducted GridEx 2011, its first electric sector-wide grid security exercise. The 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 HV transformers.⁶¹ Among other findings, the exercise determined that “utilities took appropriate steps to secure the grid.”⁶² Nonetheless, NERC recommended that “entities should ensure their response protocols address a coordinated threat,” and that it would “facilitate and support the development of updated physical security guidance.”⁶³

After the Metcalf attack in 2013, NERC conducted a second, more expansive grid security exercise, GridEx II. The exercise scenario, developed using open-source techniques, included a cyberattack on the grid coupled with a coordinated physical attack against a subset of transmission and generation assets—including HV transformer substations.⁶⁴ Among other conclusions, NERC’s after-action report stated:

While the electricity industry has experienced occasional acts of sabotage or vandalism, a well-coordinated physical attack also presents particular challenges for how the industry restores power.... The extreme challenges posed by the Severe Event scenario provided an

⁵⁹ North American Electric Reliability Corporation (NERC), *Special Report: Spare Equipment Database System*, August 2011.

⁶⁰ North American Electric Reliability Corporation (NERC), “Spare Equipment Database,” slide presentation, NERC Industry Webinar, July 22, 2013, http://www.nerc.com/pa/RAPA/webinar/dl/SED_Presentation_July_22_2013.pdf.

⁶¹ North American Electric Reliability Corporation (NERC), *2011 NERC Grid Security Exercise: After Action Report*, March 2012, p. i.

⁶² NERC, 2012, p. ii.

⁶³ Ibid.

⁶⁴ North American Electric Reliability Corporation (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.

opportunity for participants to discuss how the electricity industry's mutual aid arrangements and inventories of critical spare equipment may need to be enhanced.⁶⁵

NERC did not publicly report details about the overall impacts to the grid or outages in particular regions due to the sensitive nature of such information. Utilities and other agencies participating in the exercise viewed it a useful tool for utilities to test their readiness and preparedness for attacks on the grid.⁶⁶

FERC “Electrically Significant Locations” Study

In early 2013, prior to the Metcalf attack, then-FERC Chairman John Wellinghoff directed FERC staff to prepare an analysis identifying critical HV substations in the North American power grid.⁶⁷ Using power flow analysis software to model the impacts to the transmission system from the loss of specific grid assets,⁶⁸ FERC staff compiled a list of “Electrically Significant Locations (ESLs)” within the grid.⁶⁹ Neither details of the ESL study methodology nor its results have been released publicly by FERC or other agencies, although some findings have been reported in the press and discussed publicly by federal officials. According to the *Wall Street Journal*, the FERC analysis identified 30 critical transformers substations; in FERC's simulation, losing nine of these substations (in various combinations) as the result of a coordinated attack reportedly was found to cause a nationwide blackout for an extended time.⁷⁰

Members of Congress were highly critical of both the *Wall Street Journal* and FERC officials for inappropriately releasing what was perceived to be highly sensitive information about power grid physical vulnerability.⁷¹ A subsequent investigation by the Department of Energy's Inspector General concluded that FERC's handling of the ESL study findings was improper.⁷² The protection of information about grid security is further discussed in a later section of this report.

⁶⁵ NERC, March 2014, p. 5.

⁶⁶ See, for example, American Public Power Association, “Physical Security and the Electric Sector,” fact sheet, February 2014, <http://www.publicpower.org/files/PDFs/PhysicalSecurityIBFebruary2014.pdf>; Matthew L. Wald, “Power Grid Preparedness Falls Short, Report Says,” *New York Times*, March 12, 2014.

⁶⁷ Federal Energy Regulatory Commission (FERC), “Second Set of Responses of the Federal Energy Regulatory Commission to Senator Murkowski's Separately Submitted Questions for the Record from April 10, 2014 Hearing of the Senate Energy and Natural Resources Committee,” May 5, 2014, pp. 12-13, http://www.energy.senate.gov/public/index.cfm/files/serve?File_id=5c3bf9d7-bb7f-4379-8f57-f58881a0b5d6.

⁶⁸ FERC staff employed the commission's Topological and Impedance Element Ranking (TIER) model to identify “significant” assets based upon undisclosed criteria. For more details of the TIER model, see Bernard C. Lesieutre et al., “Topological and Impedance Element Ranking (TIER) of the Bulk-Power System,” University of Wisconsin—Madison, prepared for the Federal Energy Regulatory Commission, August 2009, <https://www.ferc.gov/EventCalendar/Files/2009091112656-TIER%20REPORT.pdf>.

⁶⁹ Federal Energy Regulatory Commission (FERC), “Response to Senator Murkowski's Separately Submitted Questions for the Record from April 10, 2014 Hearing of the Senate Energy and Natural Resources Committee, Question 39,” May 5, 2014, p. 2, http://www.energy.senate.gov/public/index.cfm/files/serve?File_id=2826f80a-a986-45d1-9261-87b45e1d6872.

⁷⁰ Rebecca Smith, “U.S. Risks National Blackout from Small-Scale Attack on Substations,” *Wall Street Journal*, March 13, 2014.

⁷¹ Senate Committee on Energy and Natural Resources, “Landrieu, Murkowski Ask Inspector General to Examine Leaks of Grid Vulnerabilities,” press release, March 31, 2014.

⁷² U.S. Department of Energy, Office of Inspector General, “Review of Internal Controls for Protecting Non-Public Information at the Federal Energy Regulatory Commission,” DOE/IG-0906, April 9, 2014.

HV Transformer Security Standards

Several grid security guidelines or standards have been developed or proposed to address the physical security of the grid, including HV transformers. These standards have been promulgated by NERC as voluntary best practices since at least 2002, with subsequent revisions. However, in the wake of the Metcalf incident, FERC has ordered the imposition of mandatory physical security standards in 2014.

IEEE Substation Security Standard

In 2000, the Institute of Electrical and Electronics Engineers (IEEE), a technical professional society, published its first standards for electric power substation physical and electronic security. The voluntary standard addressed “security issues related to human intrusion upon electric power supply substations” and various methods to mitigate them.⁷³ The standard called for the development of security assessments and, for “high-risk areas,” increased security measures such as motion detectors, perimeter/area detection systems, security cameras, physical barriers, and posted guards.⁷⁴ However, according to the IEEE, the standard is intended to address security issues related to unauthorized access, theft, and vandalism. The IEEE states that “attacks against the substation for the purpose of destroying its capability to operate, such as explosives, projectiles, vehicles, etc. are beyond the scope of this standard.”⁷⁵

NERC Physical Security Guidance

In June 2002, NERC published its initial guidance for physical response to security alerts from the federal government. This alert system was revised in October 2002 to correspond to DHS’s new color-coded threat level system.⁷⁶ NERC’s guidance was voluntary, intended to provide “examples of security measures that electric utility organizations may consider taking, based on the Alerts issued.”⁷⁷ NERC’s guidance included 35 specific security measures for the five threat DHS levels. These measures ranged from “occasional” workforce awareness programs and annual security plan reviews during times of low threat (green) to continuous monitoring of critical facilities, potentially with armed guards, during times of highest threat (red).⁷⁸ Along with this guidance, NERC published initial guidelines for vulnerability and risk assessment to help identify critical facilities and countermeasures to mitigate threats.⁷⁹

⁷³ Institute of Electrical and Electronics Engineers (IEEE), *1402-2000 - IEEE Guide for Electric Power Substation Physical and Electronic Security*, January 30, 2000.

⁷⁴ IEEE, January 30, 2000, p. 16.

⁷⁵ Institute of Electrical and Electronics Engineers (IEEE), “P1402—Standard for Physical Security of Electric Power Substations,” web page, June 3, 2014, <http://standards.ieee.org/develop/project/1402.html>.

⁷⁶ North American Electric Reliability Corporation (NERC), *Threat Alert System and Physical Response Guidelines for the Electricity Sub-sector*, Version 2.0, October 8, 2002, http://www.iwar.org.uk/infocon/threat-levels/tas_physical_V2.pdf.

⁷⁷ NERC, October 8, 2002, p. 2.

⁷⁸ NERC, October 8, 2002, pp. 3-4.

⁷⁹ NERC, *Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment*, June 14, 2002, <http://www.esisac.com/Public%20Library/Documents/Security%20Guidelines/Vulnerability%20and%20Risk%20Assessment,%20Version%201.0.pdf>.

In November 2005, NERC published a third version of its physical security guidelines, to provide “examples of security measures that other electricity sector organizations *should* consider when responding to threat level alerts” [emphasis added].⁸⁰ Thus, while still voluntary, these measures appear to have been intended as recommendations rather than considerations as stated in the earlier versions. The 2005 document included 55 measures, including new measures and existing measures expanded or described more specifically. New measures during times of low threat included, for example, annual audits of critical facility access programs and identifying critical facility long-term and short-term security measures (e.g., vulnerability assessments and security barriers).⁸¹

The Energy Policy Act of 2005 (P.L. 109-58) mandated the implementation of electric grid reliability standards under new authority granted to the Federal Energy Regulatory Commission. FERC subsequently designated NERC as the Electric Reliability Organization certified by the commission to establish and enforce reliability standards for the U.S. electric transmission grid, subject to commission review. In 2008, FERC approved NERC’s initial reliability standards for critical infrastructure; however, these standards were developed primarily to address transmission grid cybersecurity, not physical security.⁸² Subsequent NERC standards have expanded these cybersecurity requirements.

In October 2013, NERC published its most recent revision to its physical security guidance, *Security Guideline for the Electricity Sub-sector: Physical Security Response*, providing to electricity sector members “actions they should consider when responding to the threat alerts” issued by the DHS.⁸³ Continuing its voluntary (rather than regulatory) approach to physical security, NERC’s guidance states that “each organization decides the risk it can accept and the practices it deems appropriate to manage its risk.”⁸⁴ This version of NERC’s guidance lays out 77 distinct security measures corresponding to three levels of threat: (1) Normal Operations/Best Practices, (2) Elevated, and (3) Imminent.

FERC Physical Security Best Practices

In 2013, FERC staff along with staff from the Federal Bureau of Investigation (FBI), DOE, DHS, and NERC participated in a number of meetings with utilities and law enforcement agencies to discuss immediate findings and recommendations stemming from the Metcalf substation attack. As part of these meetings, FERC staff shared with utilities a list of best practices for physical security. Although the list has not been made public, it reportedly included prescriptive security measures (e.g., outward-facing video surveillance) focused on security threats similar to that experienced at the Metcalf substation.⁸⁵ In 2014, DHS, in coordination with FERC, the ES-ISAC,

⁸⁰ NERC, *Security Guidelines for the Electricity Sector: Physical Response*, November 1, 2005, p.1, <http://www.esisac.com/Public%20Library/Documents/Security%20Guidelines/Physical%20Response,%20Version%203.0.pdf>.

⁸¹ NERC, November 1, 2005, p. 3.

⁸² FERC Order 706.

⁸³ North American Electric Reliability Corporation (NERC), *NERC: Security Guideline for the Electricity Sub-sector: Physical Security Response*, October 28, 2013, p. 1, [http://www.nerc.com/comm/CIPC/SecurityGuidelinesCurrent/Electricity%20Sector%20Physical%20Security%20Guideline%20\(Approved%20by%20CIPC%20-%20October%2028,%202013\).pdf](http://www.nerc.com/comm/CIPC/SecurityGuidelinesCurrent/Electricity%20Sector%20Physical%20Security%20Guideline%20(Approved%20by%20CIPC%20-%20October%2028,%202013).pdf).

⁸⁴ NERC, October 28, 2013, p.1.

⁸⁵ Edison Electric Institute, briefing for the Congressional Research Service, February 23, 2014.

NERC, the FBI, and industry experts, has convened another series of regional briefings across North America with utilities and law enforcement officials to follow up on the initial outreach regarding substation physical security.⁸⁶

NERC Physical Security Regulations

On March 7, 2014, FERC ordered NERC to submit to the commission within 90 days proposed reliability standards requiring certain transmission owners “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.⁸⁷ In its order FERC states that physical security standards are necessary because “the current Reliability Standards do not specifically require entities to take steps to reasonably protect against physical security attacks.”⁸⁸ According to FERC’s order, the new reliability standards must require transmission owners or operators to perform a risk assessment of their systems to identify their “critical facilities,” evaluate the potential threats and vulnerabilities to those identified facilities, and develop and implement a security plan designed to protect against attacks to those identified critical facilities.⁸⁹ The order requires 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.⁹⁰ The proposed standard 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.⁹¹ The standard 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;⁹²
- R4. Mandatory threat and vulnerability assessments for critical facilities conducted by transmission owners and operators;

⁸⁶ Gerry Cauley, CEO, North American Electric Reliability Corporation (NERC), letter to Senator Harry Reid, February 12, 2014, p. 2, <http://www.nerc.com/news/Headlines%20DL/NERC%20Response%20to%20Senators%20Letter%20-Reid%20%202%2011%2014%20v4.pdf>.

⁸⁷ Federal Energy Regulatory Commission (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>.

⁸⁸ FERC, March 7, 2014, p. 2.

⁸⁹ FERC, March 7, 2014, pp. 3-4.

⁹⁰ North American Electric Reliability Corporation (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>.

⁹¹ NERC, May 23, 2014, Exhibit A, p. 1.

⁹²A 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).

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 R5.⁹³

The proposed standard also lays out a process for compliance monitoring and assessment including audits, self-certifications, spot checking, violation investigations, self-reporting, and handling complaints.⁹⁴ The new standard would be 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 P.L. 109-58.⁹⁵

Company-Specific Initiatives

Electric utilities have long had an ongoing responsibility to ensure grid reliability, in part through operating practices and investments related to grid safety and security.⁹⁶ As the standards in the previous section suggest, there has been some level of physical security investment and an increasing refinement of grid security practices across the electric power sector for at least the last 15 years. Nonetheless, several major transmission owners have recently announced significant new initiatives specifically to improve the physical security of critical transformer substations in light of the Metcalf attack. Other utilities have included new substation security investments in broader initiatives for company security.⁹⁷ The following examples illustrate the types of security changes being proposed by these grid owners. Note that other major utilities have not publicly announced similar new security initiatives. A comprehensive review or comparison of physical security plans among all major grid owners in the United States is beyond the scope of this report.

The Tennessee Valley Authority

In February 2012, the Tennessee Valley Authority (TVA) announced that it was “realigning its operations and structure to enhance security at TVA’s non-nuclear power facilities ... focusing more of our non-nuclear security resources on our critical infrastructure,” including HV substations.⁹⁸ The realignment included ending uniformed patrols in favor of installing more security technology, and the stationing of contract guards 24 hours a day at critical facilities. Together with local law enforcement cooperation, the shift to contract guards was intended to

⁹³ NERC, May 1, 2014, Section B.

⁹⁴ NERC, May 1, 2014, p. 14.

⁹⁵ Federal Energy Regulatory Commission (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.

⁹⁶ For example, see security discussion in Con Edison, Initial Brief on Behalf of Consolidated Edison Company of New York, Inc. in Support of a Permanent Electric Rate Increase, Before the New York State Public Service Commission, November 30, 2007, http://media.corporate-ir.net/media_files/irol/61/61493/total120507.pdf.

⁹⁷ See Southern California Edison, *Safety, Security, & Compliance (SS&C): Volume 4—Corporate Security and Business Resiliency*, 2015 General Rate Case, Before the Public Utilities Commission of the State of California, November 2013, [http://www3.sce.com/sscc/law/dis/dbattach5e.nsf/0/0B9F998127246B4288257C21008148B0/\\$FILE/SCE-07%20Vol.%2004.pdf](http://www3.sce.com/sscc/law/dis/dbattach5e.nsf/0/0B9F998127246B4288257C21008148B0/$FILE/SCE-07%20Vol.%2004.pdf).

⁹⁸ Tennessee Valley Authority, “TVA Realigns Security to Enhance Protection at Non-Nuclear Assets,” press release, February 17, 2012, <http://www.tva.gov/news/releases/janmar12/tvap.html>.

provide a more persistent security presence and faster incident response at key locations. Among the security technologies reportedly deployed by TVA are “surveillance, infrared cameras, video analytics for alarm verification and assessment, virtual perimeters, card readers, [and] automated gates.”⁹⁹ TVA’s security initiatives in 2012 appear to have been motivated primarily by security concerns such as copper theft, but would be applicable to more serious security risks such as terror attacks. In February 2014, after the Metcalf incident, TVA reportedly stated that it was “intensifying efforts” to educate local law enforcement about the importance of substations, including taking police on site visits to see substations during normal operations.¹⁰⁰ The utility has also been canvassing residents near TVA property asking them to report unusual activity around grid facilities.

Pacific Gas and Electric (PG&E)

In February 2014, in response to the attack on its Metcalf substation, PG&E announced that it would be investing approximately \$100 million over three years to improve substation security. Physical security measures mentioned by the company include new perimeter barriers, shielding for certain equipment, more cameras (inside and outside the fence), and clearing vegetation. For its most critical facilities, the company is “studying advanced detection technology such as night vision and thermal imaging.”¹⁰¹ Other security measures mentioned in news reports about PG&E include enhanced lighting, 24-hour security guards, and increased patrols by local law enforcement agencies.¹⁰²

Dominion

In February 2014, Dominion Virginia Power, an operating company of Dominion, announced plans to spend up to \$500 million over five to seven years “to harden its transmission substations and other critical infrastructure against man-made physical threats and natural disasters, as well as stockpile crucial equipment for major damage recovery.”¹⁰³ Dominion reportedly began to increase substation security efforts in 2013, focusing first on substations at greatest risk.¹⁰⁴ Among the security measures identified by the utility are physical barriers, additional access control, equipment design/hardening, polymer bushing installation, additional spare equipment, and relocation of spare equipment to off-site storage areas. Other measures reportedly include dual-perimeter “no man zones” around substations and installing systems for key-card access to substation yards.¹⁰⁵ Dominion’s security plan has yet to be approved by Virginia regulators for cost recovery in electric rates.

⁹⁹ “Addressing Cyber and Physical Risks in Modern Utility Security,” *Security*, March 1, 2014, <http://www.securitymagazine.com/articles/85275-addressing-cyber-and-physical-risks-in-modern-utility-security>.

¹⁰⁰ Rebecca Smith, “U.S. Utilities Tighten Security After 2013 Attack,” *Wall Street Journal*, February 9, 2014.

¹⁰¹ Geisha Williams, Executive Vice President of Electric Operations, Pacific Gas and Electric Company, “PG&E Metcalf Attack: Gunfire on Substation Has Led to Greater Security,” *San Jose Mercury News*, April 15, 2014.

¹⁰² “PG&E to Spend \$87M on Security to Protect Large Substations from Attack,” KTVU, Oakland, CA, February 12, 2014.

¹⁰³ Dominion. “Substation Security,” fact sheet, Spring 2014, <https://www.dom.com/about/electric-transmission/pdf/substation-security-soc-factsheet.pdf>.

¹⁰⁴ Tracy Sears, “Troopers Increase Security at Virginia Substations Critical to Grid,” WTVR, March 11, 2014.

¹⁰⁵ Peter Bacqué, “Va. Power to Spend Up to \$500M on Security Plan,” *Richmond Times-Dispatch*, February 8, 2014.

Bonneville Power Administration

In its 2014 draft *Security Asset Management Strategy*, the Bonneville Power Administration (BPA) proposes approximately \$37 million in additional capital spending through FY2020 for physical security measures at approximately 60 critical transformer substations.¹⁰⁶ BPA's *Strategy* states that, over the last 13 years, the utility "has conducted hundreds of security and risk assessments using several industry accepted methodologies," and began implementing security improvements based on these risk assessments beginning in 2001.¹⁰⁷

Issues for Congress

The recent transformer substations attacks, together with federal grid security exercises, have focused attention on the vulnerability of HV transformer substations to organized physical attacks. As the electric power industry and federal agencies continue their efforts to improve the physical security of critical HV transformer substations, Congress may consider several key issues as part of its oversight of the sector.

Identifying Critical Transformers

A fundamental consideration regarding HV transformer security is a clear and stable understanding of which transformers are "critical." The USA PATRIOT Act of 2001 defines "critical infrastructure" in the most general sense as "systems and assets ... so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."¹⁰⁸ Its 2009 guidelines for identifying critical assets specifically in the electricity sector, NERC defines critical assets as those "that if destroyed, degraded, compromised (e.g., misused) or otherwise rendered unavailable would unacceptably affect the reliability or operability of the [Bulk-Power System] as a whole...."¹⁰⁹ FERC's 2014 order mandating physical security standards for the grid defines a "critical facility" as "one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System."¹¹⁰ All three definitions associate "criticality" with a failure event of national significance, although none provides a more prescriptive basis for identifying such assets.

In its physical security order, FERC does not require that a "mandatory" number of critical facilities be identified under the standards.¹¹¹ Determination of whether a specific HV transformer

¹⁰⁶ Bonneville Power Administration (BPA), *Security Asset Management Strategy*, February 2014, p. 29, <http://www.bpa.gov/Finance/FinancialPublicProcesses/CapitalInvestmentReview/2014CIRDdocuments/Security%20Full%20Asset%20Strategy%20Final%20Draft.pdf>.

¹⁰⁷ BPA, February 2014, p. 31.

¹⁰⁸ P.L. 107-56 § 1016(e).

¹⁰⁹ North American Electric Reliability Corporation (NERC), "Security Guideline for the Electricity Sector: Identifying Critical Assets," September 17, 2009, p. 1, http://www.nerc.com/fileUploads/File/Standards/Reference%20Documents/Critical_Asset_Identification_2009Nov19.pdf.

¹¹⁰ FERC, March 7, 2014, p. 3.

¹¹¹ FERC, March 7, 2014, p. 3.

is “critical” will be based on each individual asset owner’s “objective analysis, technical expertise, and experienced judgment.”¹¹² In its proposed physical security standards, NERC requires transmission owners with HV assets meeting prescriptive criteria to examine whether they *may* have critical transformers, but it is up to the owners to determine themselves if any of their assets *are* critical through a periodic risk assessment based on their own respective transmission analyses, subject to independent validation.¹¹³ Thus, grid owners could have considerable latitude in determining which of their transformer substations (if any) are critical and therefore subject to the requirements of the new standard.

Although there are many candidate transformer substations in the grid, relatively few are likely to be of national significance. As discussed above, of the numerous HV transformer substations in the United States, FERC’s 2013 power flow analysis identified only 30 as being critical to the national grid (although each of these substations may contain multiple HV transformers). Whether the number of critical transformer substations under FERC’s definition above turns out to be higher or lower than 30, it will likely be only a small fraction of the total asset base. This conclusion is consistent with FERC’s expectation that under NERC’s new standard “the number of facilities identified as critical will be relatively small.... For example, of the many substations on the Bulk-Power System, our preliminary view is that most of these would not be ‘critical’ as the term is used in this order.”¹¹⁴ Consistent with this view, the NERC working group responsible for drafting the proposed physical security standard likewise expects the number of critical facilities to be “small and that many Transmission Owners that meet the applicability of this standard will not actually identify any such Facilities.”¹¹⁵

Properly identifying which HV transformer substations are critical is a key issue. Otherwise, the electricity sector risks the possibility of hardening too many substations, hardening the wrong substations, or both. Either outcome could increase ultimate costs to electricity consumers without commensurate security benefits, and could potentially divert limited security resources from other important grid priorities (e.g., cybersecurity). Independent verification is intended to validate utility assessments of substation criticality, but the standard’s reliance on company-by-company assessments may still allow for important differences in analytic methodology or assumptions, and thus inconsistent conclusions about transformer criticality. Furthermore, company-specific studies may not align with a “top down” assessment of asset criticality like that performed by FERC in its Electrically Significant Location (ESL) analysis. Congress may examine whether company-specific assessments of transformer criticality could differ from national-level assessments and what implications, if any, such differences might have on overall grid security and company efforts to protect particular substations.

Confidentiality of Critical Transformer Information

Ensuring the confidentiality of critical infrastructure information has been a long-standing concern across all critical infrastructure sectors. It is a key reason for the establishment of sector Information Sharing and Analysis Centers (ISACs), including the Electricity Sector ISAC, discussed above. Confidentiality also factors into the administration of the industry’s spare

¹¹² FERC, March 7, 2014, p. 3.

¹¹³ NERC, May 1, 2014, p. 30.

¹¹⁴ FERC, March 7, 2014, p. 3.

¹¹⁵ NERC, May 1, 2014, p. 28.

transformer programs and other activities related to critical infrastructure. FERC has established policies for the protection of critical energy infrastructure information (CEII) through a series of orders, beginning with Order 630, issued February 21, 2003.¹¹⁶ The order (§ 27) defines CEII as information that “must relate to critical infrastructure, be potentially useful to terrorists, and be exempt from disclosure under the Freedom of Information Act [FOIA].” It also establishes procedures and responsibilities for determining what information qualifies as CEII and handling CEII requests.¹¹⁷ FERC’s 2014 order mandating physical security standards also requires procedures to ensure confidential treatment of sensitive information.¹¹⁸

Press articles in the wake of the Metcalf attacks, notably in the *Wall Street Journal*, cited specific details about FERC’s 2013 ESL analysis, reportedly from a copy of a FERC presentation obtained by the paper. Notwithstanding FERC’s orders on CEII, Members of Congress and FERC officials have expressed concern that the release of the presentation by FERC staff and the publication of details in the press potentially compromised grid security.¹¹⁹ Others reportedly have disputed this concern, including the former FERC Commissioner responsible for commissioning and presenting the ESL study findings at industry meetings.¹²⁰ In April 2014, the DOE Inspector General concluded that the FERC presentation in question “should have been classified and protected from release” and “that the Commission may not possess adequate controls for identifying and handling classified national security information.”¹²¹ The Acting Chairman of FERC has testified that the commission is adopting the Inspector General’s recommendations to improve its handling of CEII and requested additional authority from Congress for exemption from FOIA.¹²²

FERC staff may be improving the way CEII is safeguarded in response to the Inspector General’s report, but securing CEII may continue to be an issue if NERC’s new physical security regulations are approved by the commission. NERC’s regulations would require independent risk assessments by multiple grid owners and 3rd party validation of those assessments. This process, by construction, would cause considerable new CEII to be created (e.g., multiple Midwest power flow models) and shared among utilities, RTOs, and consultants in ways that may be new to the industry. Ensuring that CEII generated and transferred among these entities remains secure could require special attention. As FERC’s improper management of the ESL study information shows, having strong CEII policies in place may not guarantee that those policies will be correctly and uniformly followed—even by the agency that created them.

¹¹⁶ For an overview, see Federal Energy Regulatory Commission (FERC), “Critical Energy Infrastructure Information (CEII) Regulations,” web page, June 28, 2010, <http://www.ferc.gov/legal/maj-ord-reg/land-docs/ceii-rule.asp>.

¹¹⁷ Federal Energy Regulatory Commission (FERC), Order No. 630, Final Rule, February 21, 2003, <http://elibrary.ferc.gov/idmws/common/opennat.asp?fileID=9639612>.

¹¹⁸ FERC, March 7, 2014, p. 10.

¹¹⁹ Senate Committee on Energy and Natural Resources, “Sens. Landrieu, Murkowski Ask Inspector General to Examine Leaks of Grid Vulnerabilities,” press release, March 27, 2014; The Honorable Cheryl LaFleur, Chairman (Acting), Federal Energy Regulatory Commission (FERC), Testimony Before the Senate Committee on Energy and Natural Resources Hearing, “Keeping the Lights On—Are We Doing Enough to Ensure the Reliability and Security of the U.S. Electric Grid?,” April 10, 2014.

¹²⁰ Bobby McMahon, “Wellinghoff Says FERC Analysis of Grid Vulnerability was Public, Calls Review ‘Waste of Time’,” *Inside FERC*, March 31, 2014, p. 1.

¹²¹ U.S. Department of Energy, Office of Inspector General, “Review of Internal Controls for Protecting Non-Public Information at the Federal Energy Regulatory Commission,” DOE/IG-0906, April 2014, p. 1.

¹²² The Honorable Cheryl LaFleur, Testimony on April 10, 2014.

Adequacy of HV Transformer Protection

The electric power sector has had physical security guidelines in place for well over a decade, as discussed above. These voluntary guidelines have been updated and expanded periodically to reflect industry experience, changes in the security environment, and new technologies. Prior to 2014, however, it appears that the physical security initiatives among grid owners were focused primarily on preventing vandalism and theft (of copper wire) rather than a terrorist attack.¹²³ As the recent substation attacks in California, Arkansas, and Florida have shown, many other security measures available to grid owners were not implemented—even at critical HV substations.

A grid owner's focus on vandalism and theft may be understandable because such incidents have occurred frequently and their associated costs are tangible and well-understood. Investing in security against a terrorist attack presents a greater challenge in terms of costs and benefits. 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.¹²⁴

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.

The Metcalf incident and GridEx exercises have provided the electric sector with valuable new information about the potential threat, vulnerability, and consequence of a coordinated attack on HV transformers. Risk assessments incorporating this information presumably would justify (with or without a new NERC standard) increased security investments at critical substations to prevent intentional attacks. The recently announced voluntary spending plans at PG&E, Dominion, and BPA for HV substation security appear to reflect such risk and cost-benefit reassessments. Nonetheless, there continues to be considerable uncertainty about the risk of terror attacks on the power grid, and what measures are economically justified in addressing them. PG&E, BPA, and the other utilities announcing large security investments have already decided to make such investments, but they are in the minority. Other major owners of critical HV transformers have not publicly announced similar plans.

NERC's proposed standards for power grid physical security would 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. As FERC continues to implement its policy of regulating physical security of the power grid, Congress may examine whether company-specific security initiatives

¹²³ See, for example, Michael Wills, "Changes at Duke Energy Substations Crack Down on Copper Thieves," *WUNC Radio 91.5*, May 22, 2013; Scott Kraus, "Hit Hard by Copper Wire Thieves, PPL Fights Back," *The Morning Call* (Lehigh, PA), June 6, 2013.

¹²⁴ Electric Power Research Institute (EPRI), *Technologies for Remote Monitoring of Substation Assets: Physical Security*, March 2006, p. viii.

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.

Quality of Federal Threat Information

The power industry's physical security risk assessments rely upon information about security threats provided by the federal government, among other sources, communicated through the ISAC, during DHS and other agency briefings, or through other channels. The quality of this threat information is a key determinant of what grid owners need to be protecting against and what security measures to take. Incomplete or ambiguous threat information—especially from the federal government—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. For example, prior to FERC's physical security order, the head of NERC, which initially opposed mandatory physical security standards stated,

I am concerned that a rule-based approach for physical security would not provide the flexibility needed to deal with the widely varying risk profiles and circumstances across the North American grid and would instead create unnecessary and inefficient regulatory burdens and compliance obligations.¹²⁵

Differences in the interpretation or application of threat information, as discussed in the previous section, may be a reason why some large utilities have announced major new substation security initiatives while others have not.

Concerns about the quality and specificity of federal threat information have long been an issue across all critical infrastructure sectors.¹²⁶ Threat information continues to be an uncertainty in the case of power grid physical security. For example, some federal officials reportedly have characterized the Metcalf incident as a domestic terrorist attack, potentially a “dry run” for a more destructive attack on multiple HV transformer substations, while the FBI has stated that it does not believe Metcalf was a terrorist incident.¹²⁷ Because the perpetrators have not been identified, it is impossible to know for certain, but the ambiguity has significant implications for HV substation security going forward. Although there is wide consensus that the Metcalf attack was extremely serious, some industry analysts have opined that FERC's physical security order may be an “overreaction” to Metcalf.¹²⁸ 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.¹²⁹ Still others have expressed concern that FERC's physical security concerns

¹²⁵ Gerry Cauley, President and CEO, North American Electric Reliability Corporation (NERC), Letter to Senate Majority Leader Harry Reid, February 12, 2014, p. 2, <http://www.nerc.com/news/Headlines%20DL/NERC%20Response%20to%20Senators%20Letter%20-Reid%20%202%2011%2014%20v4.pdf>.

¹²⁶ See, for example, Philip Shenon, “Threats and Responses: Domestic Security,” *New York Times*, June 5, 2003, p. A15.

¹²⁷ Rebecca Smith, February 5, 2014.

¹²⁸ 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>.

¹²⁹ Michael Chertoff, “Building a Resilient Power Grid,” *Electric Perspectives*, May/June 2014, p. 35.

may be too heavily focused on another Metcalf-type scenario (the last threat) rather than a wider range of potential future threats (the next threat).¹³⁰

There is widespread agreement among government, utilities, and manufacturers that HV transformers in the United States are vulnerable to terrorist attack, and that such an attack potentially could have catastrophic consequences. But the most serious, multi-transformer attacks would require acquiring operational information and a certain level of sophistication on the part of potential attackers. Consequently, despite the technical arguments, without more specific information about potential targets and attacker capabilities, the true vulnerability of the grid to a multi-HV transformer attack remains an open question. As Congress seeks to establish the best policies to address HV transformer vulnerability relative to other infrastructure security priorities, understanding this vulnerability in the context of specific demonstrable threats may become increasingly important. To this end Congress may examine how federal threat information is developed and used by grid owners, and how limitations and uncertainty of this information may affect the HV transformer physical security among electric utilities.

Recovery from HV Transformer Attacks

Physical security for HV transformer substations has the primary purpose of preventing successful attacks against these critical assets within the power grid. However, in the event of a successful attack, measures to minimize its effect on the overall grid are equally important so that the loss of any particular transformer remains a local event. To this end the electric power industry emphasizes its strategy of “defense-in-depth,” which includes incident response and recovery in addition to preparation and prevention.¹³¹ Industry initiatives to enhance grid resiliency, including incident recovery programs such as the DHS recovery transformer program and EEI’s spare transformer program, contribute to the power grid’s ability to sustain a terrorist attack without widespread grid failure. Indeed, some analysts have pointed to the Metcalf incident as a successful demonstration of grid resiliency; electric service was not interrupted despite the loss of a critical substation in the San Francisco Bay area. As Congress continues its examination of physical security policy, maintaining a holistic perspective on prevention and recovery as integrated aspects of HV transformer security may help to clarify an effective balance in terms of industry investment and regulatory oversight.

Author Contact Information

Paul W. Parfomak
Specialist in Energy and Infrastructure Policy
pparfomak@crs.loc.gov, 7-0030

¹³⁰ Edison Electric Institute, briefing for the Congressional Research Service, February 23, 2014.

¹³¹ Edison Electric Institute, “The Electric Power Industry’s Commitment to Protecting Its Critical Infrastructure,” February 2014, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Critical_Infra_Physical_Protection.pdf.