Electric Grid Security and Resilience

Establishing a Baseline for Adversarial Threats

June 2016

ICF INTERNATIONAL

Disclaimer

Table of Contents

List of Tables

List of Figures

Executive Summary

Purpose

This report provides an overview of the current state of the security and resilience of the entire U.S./Canadian electric grid (the bulk electric system, as well as intermediate and smaller voltage systems attached to the grid) through data and information from publicly available sources to assist policy and decision makers. The focus is on security and resilience in the context of adversarial threats, *not* natural hazards, technological accidents, aging infrastructure, changes in capacity and demand, climate change, or any of the other important aspects of maintaining a reliable grid and ensuring national/state/local security, public health and safety, and economic stability now and in the future. The state of the security of the integrated U.S. and Canadian electric grid is dynamic, with new threats and hazards emerging even as we prevent, protect against, or minimize the impacts of known threats and hazards, and improve our ability to respond to, and recover from, incidents that occur.

Technological advancements within the grid improve reliability and capacity, but can introduce new vulnerabilities in cases where additional means of remote access are added or where redundancy is reduced. Other advancements may reduce inherent vulnerabilities in design or remove the potential for human errors. At the same time, the dependence of the public, business, government, schools, hospitals, and other critical infrastructure on reliable and secure electricity continues to grow, increasing overall sensitivity to the impacts of outages and disruptions, regardless of the cause. Ensuring the security and resilience of the electric grid is critical to both the owners and operators of infrastructure, as well as government authorities.

This report supports the prioritization of next steps in line with the roles and responsibilities of each of the concerned parties: additional research and development of new cyber and physical technology solutions, upgrading of existing systems, and so forth. This report also helps identify and connect key partners in their efforts to manage and improve security and resilience, crossing national and jurisdictional boundaries, just as the grid itself does. This interconnectedness is part of what makes securing the grid so important.

Content

Section 1 – *Overview* outlines the purpose of the report and the importance of securing the grid, and provides background information on the evolution of the grid, as well as the trends and challenges that are shaping the security needs of the grid. The report then reviews some of the overall experience with both physical security and cybersecurity events, and the lessons learned from them in **Section 2 – *Analysis of Incidents***.

Section 3 – *Physical Threats and Vulnerabilities* and **Section 4 – *Cyber Threats and Vulnerabilities*** both examine the range of threats to the grid, the sources of threats, current trends, vulnerabilities, and some of the mitigation measures and protection strategies that are being implemented to address threats and vulnerabilities. Physical

and cyber issues are addressed separately; just as physical and cyber threats and vulnerabilities are very different, so are the approaches to protection and mitigation.

However, the potential consequences of a cyber or physical event can, in some cases, be similar, and lead to comparable actions to respond to, and recover from, the incident. Thus, **Section 5 – *Consequences*** addresses the types of consequences that can result from cyber or physical events, to include momentary outages, long-term service disruptions, and widespread blackouts with cascading effects, which may, in turn, yield loss of life, danger to public health and safety, damage to property, and/or economic impacts. Insufficient reliability and physical damage are discussed, along with the greater implications of impaired or disrupted grid performance. **Section 6 – *Response and Recovery*** then addresses how the electric sector works with other impacted sectors and partners to identify what has happened, minimize further consequences, and speed recovery and service restoration—as well as manage the impacts resulting from potential outages.

Section 7 – *Roles and Responsibilities in North America* looks at the responsibilities of various federal, state/provincial, and private sector entities in securing the grid, along with some of the **specific** assignments of authorities defining their respective roles. This includes some of the major information-sharing and coordination structures that have been set up within and between the United States and Canada.

Monetary incentives provided by the federal, state and private sectors for securing the grid from both physical and cyber events are discussed in **Section 8 – *Financial and Insurance Incentives***. **Section 9 – *Issues Specific to North American Grid Security*** looks at some of the things that make the North American grid unique, while **Section 10 – *Lessons Learned From Other Nations*** identifies some of the lessons that still can be learned from international experiences with physical and cyber events, as well as from other hazards, because some of the prevention, protection, or mitigation approaches used transcend the uniqueness of the grid and the nature of the threat/hazard.

Section 11 – *Conclusions and Next Steps* (see below) synthesizes the information from the rest of the report into a small number of overall observations and potential next steps. Additional information on current and planned government and industry actions can be found in **Appendix A**. Issues relating to privacy and cybersecurity are found in **Appendix B**.

Conclusions and Next Steps

Concerns about the security of the electric grid are widely recognized and shared. The fundamental issue at stake is to determine next steps for improving grid security—and how to prioritize these steps among all of the other issues that face the industry.

- **Additional threat and risk information.** Utility owners and operators, whether investor-owned, municipal, or cooperative, generally are responsible for making system improvements. However, without timely and specific information on the ways in which equipment could be damaged or disrupted by adversarial threats, it is difficult for them to properly prioritize changes, upgrades, and mitigation efforts that could improve physical security. Utility executives are now understanding the business impact of cybersecurity, making it easier to justify improvements, at least in

some cases. Actionable threat and risk assessments are needed to optimize owner/operator investments in both new technology and the replacement of aging infrastructure to improve security. These investments also need to be appropriately valued by state public service commissioners when they evaluate rate cases.

- **Integrating cyber-physical expertise.** The integration of cyber and physical systems is making major improvements in the ability to monitor and operate the grid and offering improved protection, but at the same time it is also introducing new vulnerabilities. To reduce existing vulnerabilities and minimize the introduction of new ones, we must integrate cyber and physical expertise into all stages of the research-develop-build-operate continuum. More integration is needed not just when new technology is introduced, but also when existing systems are upgraded or repaired because such changes can introduce unrecognized vulnerabilities if both overall systems and components are not evaluated before changes are made. Increased communications between technology developers, suppliers, integrators, and buyers on how the systems will be used, could help improve their understanding of security implications and, therefore, result in better solutions.
- **Understanding interdependencies.** Communications and coordination are important capabilities for identifying and understanding interdependencies and cross-sector work at the local, regional, and national levels. Convening regional webinars, taking advantage of existing industry and state government meetings, working with fusion centers, and conducting tabletop exercises (with coordinated follow up) are all ways to increase the identification and understanding of interdependencies, particularly about new infrastructure that may depend on and impact the grid and vice versa.
- **Research and development.** Significant research is underway on the design and development of new and improved grid technologies, much of it driven by investments to increase reliability, improve operational efficiency, and accommodate changing generation sources. Two areas warrant additional attention, both of which were noted in the Energy Sector-Specific Plan:[1]
  - A comprehensive framework for interdependency modeling and simulation to help (1) integrate the multiple and disparate models, tools, and simulations that already exist for different infrastructure; and (2) facilitate cross-sector analysis to address the threat assessment, protection, mitigation, response, and recovery issues associated with interdependencies.
  - Additional tests and studies on the impact of geomagnetic disturbances, electromagnetic pulses (EMP), and other physical threats on critical grid components, including large power transformers (LPTs) and bushings—or greater sharing of the results of previous tests and studies with industry if they are sufficient.

    In addition, the U.S. Department of Energy (DOE) is leading numerous research and development projects for both physical and cybersecurity, as shown in Table A-2. These projects span improvements in design, system architecture, communications, risk management tools, and training and exercises.

    Long-term research and development is needed to make grid technologies more resilient through more modular designs that support quick(er) replacement, more flexible and adaptable designs that speed recovery, self-healing systems to minimize outages and damage, and so forth. There is also a need for research

and development to enhance response to, and recovery from, adversarial incidents (as well as other types of incidents).

Significant cybersecurity work is also underway through DOE's Cybersecurity for Energy Delivery Systems (CEDS) program designed to assist the energy sector asset owners (electric, oil, and gas) by developing cybersecurity solutions for energy delivery systems through integrated planning and a focused research and development effort. CEDS co-funds projects with industry partners to make advances in cybersecurity capabilities for energy delivery systems.

Overall, it will take significant additional investment to outpace threats; this cannot be done by government alone, so government should explore policies to reduce barriers to industry investment in grid security.

- **Reducing institutional barriers.** Numerous institutional barriers are still impacting vulnerabilities, response and recovery options, and outage durations. The implications of the following on security and resilience for adversarial incidents need to be further examined so that barriers can be reduced when and where necessary: restrictions on switching fuels for electricity generation, changes in communications between electric and gas utilities due to deregulation, and limited pipeline networks in certain regions. Building trusted relationships on the state and federal levels is also key.
- **Prioritizing recommendations.** DOE, Natural Resources Canada, and the electricity industry as a whole are inundated with recommendations for research, studies, and actions on a broad range of issues, including EMP, climate change, severe storms, LPTs, cybersecurity, distributed energy resources, renewables, the smart grid, physical attacks, earthquakes, insider threats, and others. Many of these issues also impact the security of the grid, either directly or through the changes that would occur to make the grid more reliable. Rationalizing and prioritizing all of the different recommendations or groups of recommendations, even at a coarse level, could allow for the optimization of limited resources. There will never be perfect information and it is not possible to protect against every threat and hazard, but a measured approach based on risks and consequences would add clarity to the current confusion, where every issue is the most important issue. More focus on the key recommendations can hopefully also help guide further regulations to ensure that they are focused on areas with agreed-upon gaps as current regulations are more fully implemented.
- **Working on cost recovery and insurance mechanisms.** Cost recovery for security and resilience improvements is very much an area of active discussion across government and industry, and it needs to be part of an all-hazards context, just like the prioritization of recommendations. Security investments are critical to a secure and resilient grid, but they cannot overwhelm local utility rates. Close working relationships between federal and state regulators, and federal standard-setting bodies, will help achieve greater consistency in cost oversight.

  As discussed in Section 8, the available insurance options are limited and are still evolving. The recent report by Lloyd's on the implications of a cybersecurity event on the United States provides insight into the changes needed in insurance for cybersecurity events, but many of the same issues pertain to insurance for widespread physical security events, such as EMP. Interestingly, the report points out the need for innovative collaborations drawing on multidisciplinary expertise, as

mentioned earlier in this section, to develop new insurance products. Better data and modeling are also needed, including finding a means to share anonymized data on the frequency and severity of security events.[2]

1. Overview

The state of the security of the integrated U.S. and Canadian electric grid is dynamic, with new threats and hazards emerging even as we prevent, protect against, or minimize the impacts of known threats and hazards, and improve our ability to respond to, and recover from, incidents that occur. Technological advancements within the grid improve reliability and capacity, but can introduce new vulnerabilities in cases where additional means of remote access are added or where redundancy is reduced. Other advancements may reduce inherent vulnerabilities in design or remove the potential for human errors. At the same time, the dependence of the public, business, government, schools, hospitals, and other critical infrastructure on reliable and secure electricity continues to grow, increasing overall sensitivity to the impacts of outages and disruptions, regardless of the cause. Enhancing the security and resilience of the electric grid is critical to both the owners and operators of infrastructure and to government authorities.

1.1. Purpose

This purpose of this report is to provide an overview of the current state of the security and resilience of the entire U.S./Canadian electric grid (the bulk electric system, as well as intermediate and smaller voltage systems attached to the grid) through data and information from publicly available sources to assist policy makers. The report deliberately does not focus on the practices of individual utilities. The focus is on security and resilience in the context of adversarial threats, *not* natural hazards, technological accidents, aging infrastructure, changes in capacity and demand, climate change, or any of the other important aspects of maintaining a reliable grid and ensuring national/state/local security, public health and safety, and economic stability now and in the future. The state of the security of the integrated U.S. and Canadian electric grid is dynamic, with new threats and hazards emerging even as we prevent, protect against, or minimize the impacts of known threats and hazards, and improve our ability to respond to, and recover from, incidents that occur.

For the purpose of this report, physical security is defined as securing the electric grid against physical attacks by individuals or groups intent on damaging, destroying, disrupting, or removing (e.g., copper theft) components of the electric infrastructure. Likewise, cybersecurity involves securing the grid against cyber attacks by individuals or groups intent on theft, loss, or corruption of data, or damage, destruction, or disruption of cyber infrastructure and/or grid equipment. Both physical security and cybersecurity events, if not properly mitigated, could result in periods of disruption to local or regional electric services and subsequent impacts on public health and safety, the economy, and national security.

To manage and improve security and resilience, key partners and the connections between them have to cross national and jurisdictional boundaries, just as the grid itself does. This interconnectedness is part of what makes securing the grid so important. The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience,[3] along with Canada's National Strategy for Critical Infrastructure,[4] address the importance of the dependencies of other infrastructure sectors on both energy and communications systems, noting that these two sectors are uniquely critical due to their enabling

functions for the critical operations of the other sectors. This dependence exists under both normal conditions and during physical security and cybersecurity events, adverse weather events, and other disruptions.

1.2. Background

The grid is comprised of a complex mix of individually operated, but interconnected, utilities that may be investor-owned, municipal, cooperative, state-authorized, provincial, or U.S. federal. These owners and operators have the primary responsibilities for the operation and security of the grid. The owners and operators implement mitigation and protection measures to improve security and lead their response and restoration efforts. Industry works very collaboratively internally and with government agencies, the national laboratories, academia, and others to share information, identify best practices, and conduct research and development efforts to improve security and reliability. The government provides guidance, sets standards, promotes cross-sector coordination, conducts analyses, funds research and development, investigates incidents, promotes enhanced security, and works with international partners.

At a systems level, generation, transmission, and distribution are the critical functions of the grid. Electricity is created at power generating stations, then transported across high-voltage transmission lines, and then distributed over lower voltage lines to residential and business customers. Transformers at generating stations increase the electric voltage for more efficient transport and then reduce the voltage at substations to deliver power to customers. Generation and transmission components, and their associated control systems, make up the bulk power system.[5] Figure 1 shows the past, present, and future of the electric grid, illustrating changes in both generation sources and the operating technologies used to control the grid.

1.2.1. Changes impacting the grid and its components, assets, and systems

The grid itself is evolving in many ways as new technologies become available to improve system performance and capabilities, including third-party technologies, and as generation sources change. Summaries of some key trends appear below; more details on the impacts of these changes can be found in later sections of this report.

- **New sensors and grid control technologies.** Beginning in the 1970s, the previously electromechanical-based grid started automating many manual processes. As technology improved, grid operators introduced the use of automated controls and, in some cases, automated decision making became more widespread.[6] One particular recent technological advancement is a result of the application of synchrophasors, which allow 30 measurements per second of voltage, current, and frequency, while conventional monitoring technologies take measurements every 4 seconds. Such measurements allow a broader understanding of the conditions across the grid, which can assist in diagnoses of emerging problems and appropriate remedial actions, potentially avoiding serious impacts. They support wide-area management, real-time operations, power system planning, forensic analysis, and

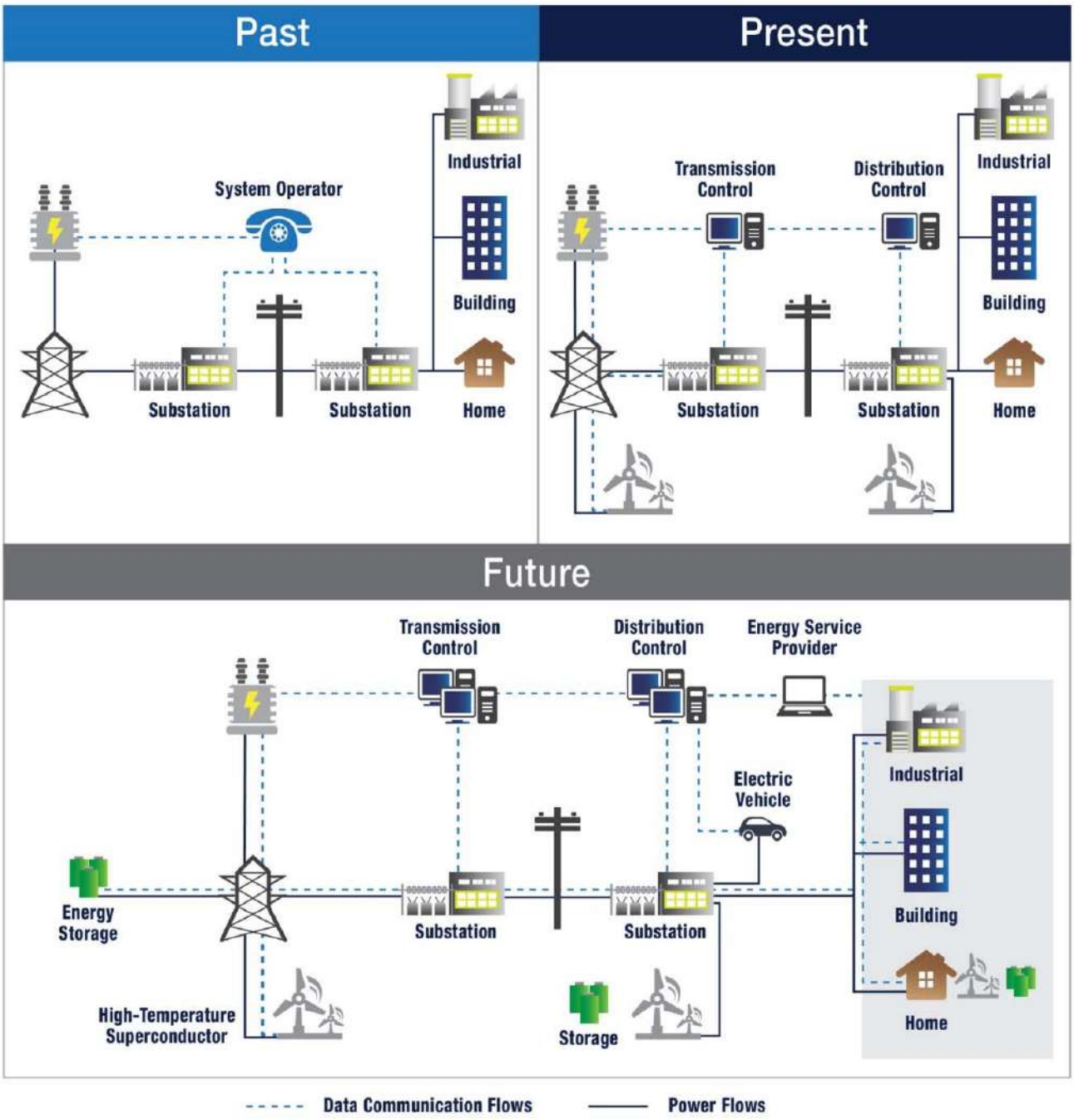


Figure 1: Past, Present, and Future of the Electric Grid

Source: European Network and Information Security Agency, *Smart Grid Security*, Annex I: General Concepts and Dependencies With ICT, 2012, https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/ict-inderdependencies-of-the-smart-grid.

further enabling the smart grid. Synchrophasors also offer the level of data needed to monitor and integrate intermittent power sources, such as solar, into the grid by allowing operators to dampen and stabilize frequency oscillations.[7] Advanced sensors and controls allow operation with reduced margins. In turn, this results in more economical operations, but can reduce the capacity for handling problems as they arise.

- **Information and communications technology/electricity interdependence.** To further increase the ability to control and monitor the grid during both routine operations and emergency conditions, information and communications technology (ICT) is becoming even more integrated into the grid and its operations. ICT supports increased observability of the systems within the grid by allowing more real-time awareness through sensors, and the ability to collect and analyze more data faster. The advanced metering capabilities of ICT allow greater understanding and control of the grid, but also create vulnerabilities, due to increasing dependence on monitoring devices. ICT has improved the operations of the grid within and across regions.
- **Increased reliance on natural gas.** Traditional fuels allow for onsite reserves, such as onsite storage of coal, adjacent rivers or reservoirs for hydro, or the long-term use of nuclear sources before refueling is required. The use of natural gas for electricity generation has increased in recent years, and natural gas is becoming the largest fuel source for generation capacity based on data for both 2016 (through February) and the usage from March 2015 through February 2016.[8] When compared with coal, natural gas is a preferred fuel due to environmental considerations and because of abundant production, while coal units are being retired and coal capacity has declined in recent years.

  The North American Electric Reliability Corporation (NERC) notes that "for some electric utilities, gas generation will begin to serve baseload, intermediate load, and peaking load requirements, whereas historically gas-fired generation has been used almost exclusively for intermediate and peaking loads,"[9] In addition, "natural gas prices reached a 17-year low in early March, making it less expensive than coal when adjusting for relative power plant efficiency."[10] However, natural gas typically is supplied by pipelines with no onsite storage. The growing dependence of electricity generation on a source without local storage capability makes the electric grid vulnerable to threats to that generation source, specifically natural gas generation and transport.[11]
- **Role of distributed energy resources and renewables.** The increased role of distributed energy resources (DER), including storage and some advanced renewable energy technologies, is also driving the growth of the intelligent grid. Changes in operating protocols and grid designs will be needed to handle the two-way flow of power resulting from DER, and the intermittent availability of renewable resources will need to be properly planned for and managed. Advanced communications and monitoring technologies are needed to ensure stable grid operations and to improve the situational awareness of operators.
- **Increased societal dependence on electricity.** Electricity is becoming even more fundamental to our daily life and the health of the economy as individuals rely more and more on cell phones, tablets, computers, and other powered devices and appliances; businesses implement greater use of advanced monitoring and control

systems, as well as data collection, Internet sales, and daily financial transactions; and electric vehicles become more popular. Customer sensitivity to outages increases with increased dependence on electricity, although the resilience of various communities to outages from severe storms indicates that there is a lot of resilience in our communities and infrastructure.

- **Continued changes in market structure and grid governance.** On top of all of these other trends, the market structure continues to change from vertically integrated utilities owning generation, transmission, and distribution systems to the increased use of independent system operators (ISOs), who operate open-access transmission systems independent of generation. Regional transmission organizations (RTOs) then administer the transmission grid on a regional basis throughout North America.[12] Other market changes include demand response to maintain reliability during periods of market stress, scarcity pricing, capacity performance using penalties to ensure that commitments are met, and changes in the membership of different power pools.[13] Other changes include the increased participation of consumers in the selection of electric providers and home- or business-based electricity generation, blurring the lines of transmission and distribution (see Figure 1).

1.2.2. Increasing sophistication in threats

Increased reliance on innovative technologies has also led to an increase in interdependencies between the electric grid and all other critical infrastructure sectors. Reliable operation of the grid is then more critical because a disruption or loss of function can directly affect the security and resilience of other critical infrastructure sectors. The components, assets, and systems making up the grid also depend on the functions of other sectors, such as communications, transportation, water, and financial services. Loss of these functions can adversely impact the functioning of the grid.[14] Both physical security and cybersecurity events may be targeted at one sector to impact another. Numerous studies have shown the importance of understanding interdependencies to inform system design and response and recovery planning.

Numerous reports find that there will be increased use of drones and other aviation technologies for physical security events to thwart various security measures, particularly as these devices become more readily available to consumers, easier to use, and less expensive. The capabilities of drones continue to increase, now including microphones and infrared/night vision.[15]

While ICT continues to play an important role in the more efficient operation of the electric grid (and other infrastructure), these integrated systems are making security across infrastructure more complex and increasing the number of potential vulnerabilities due to increased access pathways. Cyber incidents are likely to increase over the next decade, due in part to the attractiveness of internet-connected systems, and energy systems are among the most vulnerable.[16]

Cybersecurity events on the grid are of significant concern, given the increased deployment of smart grid technologies and other forms of intelligent controls and industrial control systems (ICS). Increased use of advanced controls increases the

vulnerability to both loss of capability due to malware and the hostile takeover of operations. Additionally, there is the potential to merge cyber and physical events.

Meanwhile, cybersecurity events targeting the energy sector are already occurring. One report notes that 53 percent of the more than 200 cases of hacking events handled by DHS between October 2012 and May 2013 were on the energy sector, which includes both the electricity and oil and natural gas subsectors.[17] The report notes that the majority of these involved attacker techniques such as watering hole attacks, SQL injection, and spear-phishing attacks.

Additional changes in threats are discussed in Sections 3 and 4.

1.2.3. Representative grid security efforts

Numerous ongoing efforts across all levels of government and the private sector are described throughout this report (see Sections 3–8 and Appendix A) and include standards, collaborative government-industry activities (both ongoing and special projects), and industry-driven programs (such as equipment spares) and associations. Just a few efforts and programs are summarized below to provide an indication of the range of activity underway.

Industry Practices

The grid is complex and extremely diverse in the size, type, and age of its various components, systems, and control technologies. While this diversity helps booster the grid's resilience to attack as few security events will impact all of the different components on the grid, it also increases the difficulty of having the appropriate spare equipment on hand, especially for very large power transformers. To counteract this, utilities have been voluntarily signing up with companies that will own and securely maintain critical, long lead time equipment and then help to get that equipment where it is needed.[18] Additionally, utilities are trying to reduce the types and diversity of sizes of transformers to minimize the types of equipment that might need to be replaced after an incident.[19]

Federal Bulk Electric System Standards

NERC's standard on physical security (CIP-014-2 – Physical Security) is intended to help asset owners manage the security risks of critical transmission stations and substations (and their primary control centers) from physical security events that could lead to damage and significant impacts. One of the requirements under the standard calls for a physical security plan that includes both resilience and security measures, and a timeline for executing the physical security enhancements and modifications specified in the plan.[20] In addition, there are 12 NERC critical infrastructure protection (CIP) standards covering various aspects of physical security and cybersecurity that are subject to enforcement, or pending a regulatory filing, 17 more are subject to future enforcement;[21] these standards are mandatory throughout the United States and in most provinces in Canada.

Om the cybersecurity side, NERC is encouraging more companies to adopt Critical Infrastructure Protection (CIP) version 5, which has expanded the scope of cyber assets that power and utility companies must monitor.[22]

Along with its many different standards, the National Institute of Standards and Technology (NIST) is collaboratively working with stakeholders and partners to build a solid framework and roadmap for smart grid interoperability standards.[23] Such guidelines should improve both operations and response and recovery efforts. The structure of NIST reflects the changes within the grid as NIST's Engineering Laboratory now has a Smart Grid and Cyber-Physical Systems Program Office.

State Efforts

The National Association of Regulatory Utility Commissioners (NARUC) released *Cybersecurity for State Regulators With Sample Questions for Regulators to Ask Utilities* in 2012 to assist state regulators in understanding and promoting cybersecurity, particularly for the electric grid.[24] NARUC has many additional efforts addressing physical security or cybersecurity.

Individual states also undertake studies after key events that can be useful for improving grid security. The New York State (NYS) Ready and NYS Respond Commissions identified three overarching themes to guide the State of New York in preparing for the future[25] and these observations can be readily adapted to both cyber and physical threats:

- Information: Obtaining and sharing reliable and timely data.
- Inter-connectedness: Breaking down sector silos (or understanding interdependencies).
- Informed decision making: An expanded definition (beyond just having the necessary basis for a decision) that also involves being transparent and clear about how critical decisions are made and the respective roles of government and other partners.

In addition, state and local fusion centers also help coordinate two-way information sharing across all levels of government and owners and operators to help ensure that the proper actions can be taken in response to both threats and actual events.

Joint Government-Industry Efforts for Cybersecurity Preparedness

Efforts to increase the electric sector's awareness of cybersecurity risks, enhance coordination and information sharing, and identify potential protection actions include:

- The U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability (DOE/OE) and industry have co-funded a public-private partnership to facilitate the timely two-way sharing of both classified and unclassified threat information, and to develop situational awareness tools to improve the protection of critical assets. Known as CRISP, the Cybersecurity Risk Information Sharing Program leverages threat analysis techniques developed by DOE, advanced sensors, and DOE's participation in the National Intelligence Community to provide actionable information to energy partners.[26]
- DOE/OE and industry also collaborated on the Electricity Subsector Cybersecurity Capability Maturity Model (C2M2) to help energy sector owners and operators

evaluate, prioritize, and improve their cybersecurity capabilities, and allow for a better overall assessment of the cybersecurity posture of the energy sector.[27]

- The Smart Grid Investment Grant (SGIG) program also recognized and promoted cybersecurity preparedness. Funding recipients included investor-owned utilities, public power utilities, and cooperatives, and each project that received a grant had to develop a cybersecurity plan. The preparation of the plans both increased awareness of cybersecurity risks and drove the implementation of cybersecurity protective actions.[28]
- Canada has hosted six workshops on ICS, bringing together more than 150 critical infrastructure stakeholders and aiming to assist Canada's critical infrastructure owners and operators better secure their most critical ICS and information technology (IT) assets. The 2016 workshop featured presentations on threats and vulnerabilities, incident management and forensics analysis, architecture and operations best practices, emerging research, security technologies and standards, and procurement standards and best practices.
- Several collaborative partnerships have been established, including the Electricity Subsector Coordinating Council. This council works on a variety of information sharing, risk management, mitigation, and protection efforts.

1.2.4. Implications

Collectively, the changes in the threat environment and the grid itself illustrate the importance of continuing to design and build security into improvements made for reliability and operability. Although the diverse nature of grid assets, components, and systems today may make it harder to attack, this diversity may also increase the difficulty of applying security fixes after the fact and implementing appropriate resilience strategies, such as redundancy, increased reliability, appropriate spares, and both cyber and physical mutual-aid agreements.

In addition, a recent study by Lloyd's highlights three attributes of cyber risk that are significant to the development of security (and insurance) solutions:[29]

- Cyber connections create a systemic exposure that can result in widespread impacts.
- The intangibility and time delay of many cybersecurity events make understanding the impacts difficult.
- The nature of the threat is always changing as attackers identify new vulnerabilities.

2. Analysis of Incidents

2.1. Physical Security Events

2.1.1. Overview

Physical security events take on many forms, involve different levels of coordination and planning, and may be carried out by individuals or groups. Section 3 talks about some of the classes of threats and actors. To date, most incidents in the United States and Canada have been relatively minor in terms of their consequences (e.g., vandalism). As an illustration of this, DHS analyzed malicious incidents conducted against the electric grid and found that there were 65 malicious incidents that the Electric Emergency Incident and Disturbance Reports (OE-147) grouped as sabotage (1 incident), physical events (27), and vandalism (37) for October 2013 through September 2014.[30] The most severe of these categories is typically sabotage, which is more deliberate and well planned than other incidents, and often has an insider component. Physical events may stem from some sort of grievance and typically have moderate impact. Vandalism is random and opportunistic, and usually has the least impact, although there are extreme exceptions to this. The damage to electrical power systems can range from copper theft where the impacts on the system are not a concern by the thieves, to planned events where impacting grid operations is the intended purpose. The most significant of the events analyzed by DHS are shown in Figure 2, and represent all three types of incidents. The outages do not necessarily denote loss of customer service.[31] To date, outages from physical events are on par with, or less significant than, outages caused by natural events.

2.1.2. Selected events

A number of actual events are described below by the part of the grid that was targeted. These incidents generally resulted in relatively minimal damage and outages, demonstrating the resilience of the grid to physical security events, as well as other causes of damage.

Substations and Transmission Lines

Large power transformers (LPTs) are key components of the electric bulk power system that have long lead times (up to a year) to manufacture and deliver. The U.S. electricity industry has had multiple experiences with the loss of a single transformer, but the United States has never simultaneously had to replace multiple LPTs.

- The largest and most consequential physical event to date was on Pacific Gas & Electric's (PG&E) Metcalf Substation (500 kilovolts [kV]) in California when it was attacked in April 2013 by snipers,[32] although no loss of service to customers resulted due to rerouting power from other parts of the grid. Not only were parts of the substation put out of service for nearly a month, but the sophistication of the event caused concern in the industry as it was seen as a precursor to an even greater

Figure 2: Twelve-Month Timeline of Significant Events (2013–2014)

Source: U.S. Department of Homeland Security, *Malicious Incidents Against the Electrical Sector, October 2013 – September 2014*, March 2015.

physical security event on the grid. The event is widely regarded as a professional job for several reasons: moments before the event, communication lines were cut; the attackers used military-style weapons and left nearly 100 bullet casings; and the oil cooling systems were targeted, causing 52,000 gallons of oil to leak and resulting in 17 large transformers overheating and being shut down. The event resulted in $15 million in damages, and took PG&E 27 days to repair equipment and bring the substation back online.[33] Seemingly, no LPTs had to be replaced.

Since the event, PG&E has made efforts to prevent such an event through measures taken to enhance the security of critical substations across its service territory, which include:[34]

- Employing security guards to provide 24/7 coverage.
- Trimming back undergrowth around substations to remove potential hiding places.

  - Constructing fencing and shielding to obstruct the view and protect critical substation components.
  - Enhancing camera technology.
  - Increasing lighting.

    There has been debate about the success of the event considering that it did not cause an outage.

- Two physical security events took place in Crimea in November and December 2015. The first event was blamed on sabotage and the saboteur(s) was not identified. Power from Ukraine was only partially restored after a few weeks and Russia boosted its share of the power supplied to the region, including flying in emergency generators. The second event was an explosion that blew up transmission towers that disrupted power to at least 25 percent of the residents of Crimea by cutting off the only functional high-voltage line providing electricity to Crimea. In Sevastopol, rolling blackouts were used to save power. There are significant political issues between Ukraine and Russia regarding future sources of electricity to the region. Russia wants to complete two more undersea cables so that Crimea is independent from Ukrainian electricity.[35]
- In 2014, an incendiary device was attached to a diesel fuel tank at the Valencia Substation in Arizona. The device was described more as "a big match than a grenade or explosive" by the Arizona Department of Public Safety bomb squad.[36] The attempt was largely unsuccessful because it only caused a small leak and charred the surface of the tank. Officials described the event as a "crude" attempt, but saw it as a precursor to more serious physical security events on the grid.[37]
- There were a series of physical security events targeting grid equipment in Arkansas from August through October 2013.[38] These were executed by one individual.
  - The initial event was a downed Entergy 500kV transmission line. The perpetrator climbed a 100-foot tower, cut the line, and removed several bolts at the base of the tower. There were no injuries or power outages.
  - An Entergy 500kV substation was set on fire and a message was left at the entrance, stating "You should have expected U.S." The fire consumed the substation control house; there was no interruption of electrical service.
  - The final event left 10,000 First Electric Cooperative customers without power when a utility pole was pulled down by a tractor, downing a 115kV transmission line.

    A single individual was arrested and charged with this set of physical security events on the transmission grid.

- In 2005, a rifle event at a Progress Energy substation in Florida ruptured a transformer oil tank, ultimately causing an explosion and local blackout.[39]
- In October 1997, someone used a key to illegally enter a substation in San Francisco and opened 39 control switches. While this did not damage the LPT, it did shut down the substation, leaving 126,000 customers without power for up to 3.5 hours.[40]

None of the events caused large or extended outages, but these cases highlight the vulnerability of the grid to physical security events orchestrated by a single motivated individual.

Transmission Towers

The accessibility and remoteness of transmission towers and lines make them a vulnerability of concern as well, although they typically can be restored quickly, as evidenced when damaged by ice storms and hurricanes. Malicious damage to insulators (by shooting at them) and sabotage are ongoing concerns as well. "In October 2003, a saboteur removed support bolts at the base of twenty high-power transmission towers in the Pacific Northwest. The suspect surrendered to police on November 2, 2003, and later admitted to the crime; he was sentenced to 27 months in prison and ordered to pay $37,000 in restitution. At his sentencing, the saboteur said he was trying to point out the power system's vulnerability."[41]

Natural Gas Supply

Events targeting natural gas supply can potentially disrupt electric grid operations as well. There were five accidental fires or explosions between 1995 and 1997 on the TransCanada pipeline, which transports gas to the New England region. While not physical security events, these events indicate the vulnerability of gas transmission lines were a physical security event perpetrated in an attempt to achieve similar results. The most significant event was an explosion in Manitoba that took out six parallel pipelines making up the TransCanada system plus two electric generators at a nearby compressor station. Two lines were returned to service the same day as the incident, three lines were not restored for more than a week, and it was roughly a month before the remaining pipeline and one generator were back in service. All interruptible service on the system was impacted and TransCanada had to stop roughly one-third of its firm supply commitments.[42]

2.2. Cybersecurity Events

2.2.1. Overview

There have been an increasing number of cybersecurity events to the U.S./Canadian electric subsector, although, so far, these have been largely unsuccessful. Methods of typical cybersecurity events impacting the grid have been mainly limited to gaining access to networks through phishing emails, or infecting flash drives with the hope that they will be connected to a network.

As an example, data from the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) show that 53 percent of malware events *reported* for October 2012 to May 2013 were made on the energy sector, including both electricity and oil and natural gas; note that many events are not reported. The overall count of reported incidents was roughly 200, but the large percentage is telling.[43] Data from Alert Logic showed 8,840 incidents for energy companies in less than 5 months of 2013.[44]

2.2.2. Selected events

While attacks on the US grid and affiliated systems have had limited consequences to date, attacks elsewhere in the world on energy systems may be seen as indicators of what is possible.

- In 2013, a major Florida utility experienced a distributed denial-of-service event that shut down payment systems.[45]
- Reports state that, in 2013, Iranian-backed attackers accessed control system software for oil and gas pipelines.[46]
- A cyber campaign involving BlackEnergy malware has compromised numerous ICS environments since 2011. Targets are users of Internet-connected human-machine interface products, including General Electric Cimplicity, Advantech/Broadwin WebAccess, and Siemens WinCC.[47] There has been concern that the purpose of BlackEnergy is reconnaissance before an event.[48]

The most sophisticated and most successful cybersecurity event in the electricity sector to date occurred outside North America, on the Ukrainian electric grid, providing insight into possible future attacks. On December 23, 2015, Ukraine experienced widespread power outages resulting from remote cybersecurity events at substations where the attackers opened breakers and locked out system operators.[49] The impacts of the event are shown in the box on the following page.

The magnitude of the outage, the level of sophistication, and the perpetrator are all important to consider. The size of the outage was relatively minimal, but it was the most successful and sophisticated event on an electric grid yet, in addition to having political ramifications because of the potential implications if it were an event launched by Russia. The rapid power restoration occurred due to field staff manually reclosing breakers at affected substations.[50]

Ukraine Cybersecurity Event

- Total of six organizations were compromised, three of which were regional electric distribution companies.
- Seven 110kV and twenty-three 35kV substations were disconnected.
- “Synchronized and coordinated, probably following extensive reconnaissance.”
- Wiped the computers using KillDisk malware.
- Infected and corrupted equipment, leaving it inoperable.
- Overwhelmed the call center with a denial-of-service event to prevent people from reporting outages.
- Left 225,000 without power for 1 to 6 hours.

2.3. Lessons Learned

Over recent years, more frequent and increasingly sophisticated security events targeting the grid from both a physical and cyber perspective have raised concerns about the security of the electric grid, sometimes based on media attention rather than fact. So far, most physical security events have been simple or crude events targeting electric grid infrastructure that caused minimal outages. While no events so far have been catastrophic, they make the vulnerabilities of the grid clearer to the public and other stakeholders. In the case of a more sophisticated physical security event, like the one on the Metcalf Substation in California, it is evident that there was potential for more significant damage. Long and widespread outages were avoided by rerouting the power; however, it took weeks to repair and bring the substation back online.

Industry's response to an increasing number of physical threats has been to invest in better security systems and barriers to protect critical infrastructure. Additionally programs like SpareConnect have been developed, to allow bulk power system asset owners and operators to network with one another in order to facilitate the sharing of transmission and generation step-up transformers and related equipment in the event of an emergency or other non-routine failure.

The incident in Ukraine reinforces the argument for secure ICS and supervisory control and data acquisition (SCADA) networks as more devices are controlled electronically and provide remote access, particularly as reports have indicated that if best practices were being followed in the Ukraine, the incident would not have been successful. The compromise of control systems could allow physical equipment to be operated with malicious intent; if also targeted during the security event, the alarm systems could fail to alert system operators to react in time or the system could be instructed to lock out the operators.[51] It was not malware or any other element of the event that caused the power outage itself, rather the outage was caused by the hijacking of the ICS through SCADA.[52] While 30 substations were disconnected, power was restored in a matter of hours through manual efforts. However, if the system had been compromised for an extended period of time during which the attackers could perform more reconnaissance, that would leave open the possibility that the attackers could remain dormant and wait for the perfect opportunity to strike again. More and more devices are being controlled remotely, which increases the range of equipment that can be operated with malicious intent. A cybersecurity event also differs from a physical security event because it can be carried out remotely from a single location and can affect multiple, far-reaching geographic locations. Cybersecurity events can be precursors to physical or combined cyber-physical security events

Another issue with cyber threats is that systems could already be infiltrated but go undetected while the intruders study the system, gathering industry data and identifying system interdependencies for the possibility of cascading failures. There are also a number of ways for intruders to gain access to the system, which raises the need for industry and government collaboration to continue to share information about cybersecurity events and identified vulnerabilities, and adopt any known best practices to prevent this type of event. Not only should efforts be made at the management level to prevent this type of threat, but training and best practices need to be communicated throughout the workforce to help spread awareness on how employees also can mitigate

risk. Section 4 of this report discusses the operational deficiencies/vulnerabilities that were identified as associated with the Ukraine event: spear phishing, remote access, control, and tools/technical.

Government lessons learned from physical security and cybersecurity events, as well as vulnerabilities and response/recovery issues pointed out through extreme storms, include the need for research (by industry and government) on the best way to harden equipment, better modeling and simulation, grid modernization, and approaches to increase cybersecurity (e.g., the Cyber Security for Energy Delivery System program); sharing physical and cyber threat information; development of a design basis threat; increasing the understanding of electromagnetic pulse (EMP) threats, vulnerabilities, and consequences; and the need for standards to help address vulnerabilities and minimize consequences (e.g., NERC CIP-014). Many of these efforts are discussed in later sections of this report.

3. Physical Threats and Vulnerabilities

This report looks separately at physical and cyber threats and vulnerabilities (this section and Section 4, respectively) as these tend to be different in origin, and may require different approaches to protection and mitigation. (In this report, threats refer to potential types of, or plans for, adversarial events or attacks; once they occur or are underway, they are referred to as physical security events or attacks.) However, consequences (Section 5) and response/recovery (Section 6) are addressed jointly for physical and cyber due to commonalities in almost all areas, with the exception of some of the direct physical damage from physical security events.

3.1. Range of Threats

The Strategic National Risk Assessment[1] (SNRA) identified three groups of threats/hazards of concern for their potential to yield nationally significant impacts to homeland security, measured in terms of economic consequences, fatalities or injuries/illnesses, or psychological impact. The assessment was used to support: development of the core capabilities and capability targets in the National Preparedness Goal; collaborative thinking about strategic needs across prevention, protection, mitigation, response, and recovery requirements; and a shared common understanding and awareness of national threats and hazards, and resulting risks across government.[53] The three groups of threats/hazards and the number of distinct types of scenarios that were evaluated under each are:[54]

- Natural hazards (9)
- Technological/Accidental hazards (4)
- Adversarial/Human-caused threats (10)

The threats within the last category that were included in the SNRA are shown in Table 1. The table focuses on non-state actors because of the mission of DHS, but state actors could pose the same threats.

Within this set of threats, the two related to cyber are addressed in Section 4. Of the rest, the ones most likely to have a direct impact on the security of the electric include: (1) aircraft as a weapon, (2) armed assault, (3) explosives terrorism attack, (4) nuclear terrorism attack, and (5) some radiological terrorism attacks. These are the types of threats discussed in this section; the remaining three are chemical or biological attacks not necessarily aimed at the electricity sector per their descriptions. It is important to recognize, however, that many natural and technological or accidental hazards could yield similar impacts, either on the grid or on the supply chain for electricity generation sources.

[1] The SNRA was conducted in support of PPD-8 on national preparedness [*Source:* U.S. Department of Homeland Security, *The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-based Approach Toward a Secure and Resilient Nation*, 2011, https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf.] PPD-8 called for the development of a National Preparedness Goal, a National Preparedness System, and a National Preparedness Report.

Table 1: Potential Adversarial/Human-Caused Security Events

Threat	Description
Aircraft as a Weapon	A hostile non-state actor(s) crashes a commercial or general aviation aircraft into a physical target within the United States.
Armed Assault	A hostile non-state actor(s) uses assault tactics to conduct strikes on vulnerable target(s) within the United States.
Biological Terrorism Attack (non-food)	A hostile non-state actor(s) acquires, weaponizes, and releases a biological agent against an outdoor, indoor, or water target, directed at a concentration of people within the United States.
Chemical/Biological Food Contamination Terrorism Attack	A hostile non-state actor(s) acquires, weaponizes, and disperses a biological or chemical agent into food supplies within the U.S. supply chain.
Chemical Terrorism Attack (non-food)	A hostile non-state actor(s) acquires, weaponizes, and releases a chemical agent against an outdoor, indoor, or water target, directed at a concentration of people using an aerosol, ingestion, or dermal route of exposure.
Cyber Attack Against Data	A cyber attack, which seriously compromises the integrity or availability of data (the information contained in a computer system) or data processes.
Cyber Attack Against Physical Infrastructure	An incident in which a cyber attack is used as a vector to achieve effects that are beyond the computer (i.e., kinetic or other effects).
Explosives Terrorism Attack	A hostile non-state actor(s) deploys a human-portable improvised explosive device (IED), vehicle-borne IED, or vessel-borne IED in the United States against a concentration of people and/or structures, such as critical commercial or government facilities, transportation targets, or critical infrastructure sites, etc.
Nuclear Terrorism Attack	A hostile non-state actor(s) acquires an improvised nuclear weapon through manufacture from fissile material, purchase, or theft, and detonates it within a major U.S. population center.
Radiological Terrorism Attack	A hostile non-state actor(s) acquires radiological materials and disperses them through explosive or other means (e.g., a radiological dispersal device or creates a radiation exposure device).

Source: U.S. Department of Homeland Security, *The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-based Approach Toward a Secure and Resilient Nation*, 2011, pp. 3–4, https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf.

DOE, the Pacific Northwest National Laboratory, NERC, and utility managers from a number of utilities have piloted a design basis threat (DBT) for physical security for the electricity sector. If successful, the DBT would be intended to help utilities understand from which threats they should protect assets.

3.2. Sources of Threats

Various groups and individuals can execute physical security events. Here is a taxonomy of actors, derived from a number of different ways to define and divide them:

- State actors: Individuals or groups whose actions are on behalf of, and sanctioned by, a country.
- Non-state actors: Other individuals or groups conducting activities based on beliefs grounded on principles of separatism, race, nationalism, political ideologies, revolution, or religion, among others. These groups may be centered in an individual country or region, or may be more widespread.
- Other groups: These could be considered non-state actors, but are more typically focused on particular issues, such as the more radical groups trying to protest abortion, protect the environment, or protect other human (or animal) rights.
- Home-grown violent extremists (HVEs): A person who lives or operates primarily in the United States (not necessarily a citizen), who advocates or engages in ideologically motivated terrorist activities in support of the objectives of a terrorist organization, without direction by that organization.[55]
- Insider threats: Employees working from inside an organization to cause damage or disruption. These individuals have one or more of the following characteristics: psychological impairment leading to disgruntlement or alienation, radicalization around ideological or religious positions, and/or criminal behavior.[56]

Understanding the types of actors and their motivations can be insightful for identifying and understanding potential threats and addressing associated vulnerabilities, as well as the means for protecting against them or mitigating them.

3.3. Trends for Physical Threats

3.3.1. Social media and new technologies are increasing the potential for security events

Terrorist organizations are increasing their international reach and impact on affiliated and non-affiliated individuals through social media, email, and other Internet-enabled platforms. Continued participation via these methods fosters interactions with other individuals with similar interests or concerns, and may eventually lead to self-radicalization and potential physical action against infrastructure, including electric infrastructure.[57] The Congressional Research Service assessment from 2013 notes that approximately 63 HVE plots or attacks (in general, not specific to the electric grid) have occurred in the United States since September 11, 2001.[58] Furthermore, from 1968 to 2010, there were 198 single actor attacks in the United States and 14 other western countries; 113 of these occurred in the United States alone.[59]

The ill-intentioned use of drones and similar devices is likely to increase as such equipment becomes more readily available to consumers, easier to operate, and less expensive. Whether deployed by a state or non-state actor, or an HVE, such aerial devices can circumvent walls, barriers, and other ground-based security measures, providing increased access to all types of critical infrastructure.[60]

3.3.2. ICT infrastructure embedded in the grid

In their study of high-impact/low-frequency events, NERC and DOE noted that "[t]he risk of a coordinated cyber, physical, or blended attack against the North American bulk power system has become more acute over the past 15 years as digital communicating equipment has introduced cyber vulnerability to the system, and resource optimization trends have allowed some inherent physical redundancy within the system to be reduced."[61] Thus, the integration of ICT has increased the interdependence between electric and communications systems and introduced new vulnerabilities. Enhancements in grid control offered by ICT has allowed utilities to optimize operations and eliminate some of the redundant equipment and systems that were previously needed to establish and maintain grid reliability. With some redundancy removed, fewer options for response to, or recovery from, an attack are available, which may be attractive to attackers if known.

3.3.3. Increased awareness of insider threats

The 2008 National Infrastructure Advisory Council (NIAC) study defined insider threats for critical infrastructure as follows:

> "The insider threat to critical infrastructure is one or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm."[62]

Insider threats exist for all companies and infrastructure. Essentially, this threat involves an employee's betrayal of their obligations and allegiances to their employer as realized through acts of theft or sabotage, workplace violence, or espionage against the company.[63] NIAC determined insider threats to be significant given their potential to cause cascading consequences beyond the attacked infrastructure.[64]

There is significant concern about a "large and growing threat of Nation-State economic espionage targeting critical technologies in U.S. critical infrastructure companies."[65] Insiders, who have been enticed or compromised by the nation-state to collect the requested information, may be used to carry out this espionage. Economic espionage threats create a greater potential for intellectual property theft, which could impact competitiveness and lead to major financial losses or provide enhanced access for subsequent physical and cyber attacks. Although critical U.S. technologies may be the primary targets of these threats, critical information on the most vulnerable assets or on ways to access critical equipment and facilities on the grid could also be at risk in these cases.[66]

A number of policy recommendations were made by NIAC to combat near-term insider threats across critical infrastructure: education and awareness, employee screening, technology policy, information sharing, and follow-on insider threat study and research.[67] Within the electric sector, the Electricity Subsector Coordinating Council (ESCC) is working to find mechanisms that will allow the sector to have employees checked

against the Federal Bureau of Investigation's (FBI) database, similar to what the NIAC study recommended.

3.3.4. Unwitting insider threats

Another category of insider threat is the unwitting insider. Unwitting insiders are the loyal employees who click on a link in a phishing email, or go to a malicious website, or find a universal serial bus (USB) drive and plug it into their computer to see what is on it, or give out confidential information to a social engineer on the telephone. The employee is not intentionally loading malware on the company network or giving away sensitive information in any of these cases and, in almost all cases, do not even realize they did so. But threat actors, especially cyber threat actors, have such good success with these methods that they often have no need for advanced sophistication in order to achieve their objectives. Continuous awareness training and a corporate culture that rewards the reporting of incidents can reduce some of the risk and improve incident identification and response times.

3.3.5. Increased concerns about electromagnetic pulse events

Recent threats to attack the United States with nuclear weapons, claims of hydrogen bomb developments, and ballistic missile tests by North Korea[68, 69] have heightened concerns over the risks of EMP attacks—whether from North Korea, Iran, China, Russia, or other countries. As described in numerous studies,[70, 71, 72, 73] successful detonation of a nuclear device at a high altitude above the United States or Canada could have both widespread and long-term effects within and beyond the electric sector. Even if particular geographic areas were not directly impacted by an EMP, damage to the grid in impacted areas could cause cascading failures in otherwise undamaged areas. A worst-case EMP attack requires both a nuclear device and a missile to carry it to high altitudes, and recent ballistic missile tests demonstrate that there are countries and organizations interested in developing the capability to carry out such attacks. Smaller EMP attacks can be carried out by pulse generators at low or no altitude.

3.3.6. Natural hazards and high-impact/low-frequency events as surrogates for threats

Significant nationwide and even multiple-country impacts can be realized from a range of natural hazards, and given the limited experience with physical threats, they can help inform the electric sector's knowledge of how threats can target inherent vulnerabilities.

Severe weather is the primary cause of grid disruptions, including hurricanes, snow and ice storms, and temperature extremes—which can both increase demands on gas and electric supplies, and directly impact grid performance through outages and damage.[74] Past experience provides guidance on the impacts of severe weather, and there are numerous after-action reports and studies that identify lessons learned and best practices.[75, 76]

High-impact/low-frequency events such as geomagnetic disturbances and catastrophic earthquakes are of concern to the electric grid. These events are similar to major physical attacks in that the grid has limited or no experience with such events. Thus, the framework for understanding and planning for such events can be helpful to managing the risks of physical attack. A joint report on high-impact/low-frequency events[77] makes numerous recommendations on managing high-impact/low-frequency events. Another resource is NERC's *Severe Impact Resilience: Considerations and Recommendations.*[78]

Similarly, Public Safety Canada's *A Guideline for Enhancing Canada's Critical Infrastructure Resilience to a Catastrophic Space Weather Event*[79] and *A Guideline for Enhancing Canada's Critical Infrastructure Resilience to a Catastrophic Earthquake*[80] provide guidance on mitigation, preparation, response, and recovery actions that may have implications for a physical attack as well. The United States has a comparable National Space Weather Strategy and an accompanying Action Plan that address the United States at large, not just critical infrastructure.[81, 82]

3.4. Vulnerabilities

Individual elements of the grid are certainly vulnerable to physical attack, given their relative openness and visibility, sometimes in close proximity to populated areas and other times unattended in rural areas. The extent to which the grid as a whole is vulnerable is less well understood, particularly as improved ICT offers ways to minimize the impacts of specific outages at the same time as it introduces new vulnerabilities. This section provides an overview of some of the areas of vulnerability.

3.4.1. Grid asset and system vulnerabilities

Generation-related vulnerabilities on the grid include events taking facilities offline, situations causing reduced gas or other fuel supplies, lack of infrastructure in certain regions, and even firm industrial commitments that reduce the ability to generate electricity. The grid is more susceptible to attacks because of decreased reliability (often associated with aging infrastructure), increased interdependencies with communications and other sectors (and their associated demands for electricity), and the increased application of unsecured ICT.

The size of LPTs makes them easy to identify and hard to protect from physical attack. While loss of a single transformer would not be catastrophic, larger scale attacks resulting in multiple LPT loss could be. Further, the extensive media coverage of LPTs, particularly their importance to transmission and their long lead times for replacement, has increased the awareness of this equipment, thereby creating greater interest in them as potential targets. LPTs can take 5–20 months or more to transport. Their cost in the millions of dollars and the diverse range of sizes and types installed at different locations make it difficult for companies to stock spares for their full range of LPTs. The logistics associated with getting replacements to a site are difficult because of their weight in hundreds of tons.[83] Also, the reliance on third-party equipment and services increases the chance of extended replacement times.

Other transmission components that are vulnerable to physical attacks include transmission lines, towers, and control centers. Transmission lines and towers are often in remote areas without much surveillance or other forms of protection. Damage to transmission towers has occurred from both weather and malicious activities, and past experience shows that the impacts are short lived and localized.[84]

As noted in a recent report from the Conference Board of Canada, half of the generation stations in Canada were built prior to 1980, and while the current rate of investment in infrastructure is higher than in any previous decade, that investment is now spread among a changing mix of generation sources (including renewable sources), new market demands, and the replacement or updating of aging assets. Up to two-thirds of investments in the electric grid are being spent to address aging infrastructure through replacement or repair.[85] While this presumably includes a number of the ICT improvements mentioned earlier in this report, these replacements are another demand for financial resources as utilities and others strive to optimize operations, increase reliability, and improve security. This same competition for resources is seen in the United States and can leave aging infrastructure in place with a potential for increased susceptibility to attacks.

3.4.2. Increased importance of understanding dependencies and interdependencies

In a study for the New York State Division of Homeland Security and Emergency Services, ICF found that vulnerabilities can arise from both intra-sector dependencies and external or cross-sector dependencies.[86] For the electric grid, examples of such dependencies can include those between assets on, or directly supporting, the grid; those across generation and transmission facilities and systems, extending into distribution systems; as well as all forms of communications. Supply chain dependencies can also create grid vulnerabilities, such as fuel dependencies (e.g., natural gas and coal) that involve other sectors, such as transportation and the oil and gas sector. Communications is another dependency that can create grid vulnerabilities.

3.4.3. System design issues

The specific configuration of different parts of the grid can potentially allow failures to cascade if there is instability, uncontrolled separation, or cascading within an interconnection. Failures can also expand as power to critical supporting infrastructure is lost. Integrated cyber and physical elements of the grid means that some select types of cybersecurity events can also result in physical damage to, or disruption of, the grid. Such an attack could first leverage the deployments of ICT and then render many of the advanced metering and control systems useless in restoring the grid or keeping damage from propagating, somewhat like what was experienced in the attack in Ukraine. There is also the potential to enhance the impact of a physical attack by launching a concurrent cybersecurity event.

System design changes can have unintended consequences in terms of introducing new physical vulnerabilities. For example, the operating procedures and technology changes needed to ensure that DER and grid-scale renewable resources can operate smoothly

within the grid introduce additional vulnerabilities. Likewise, some of the compressors along the natural gas pipelines are being switched to be powered by electricity rather than gas, but this means that a loss of electricity in one area can cut off or reduce the gas supply to another area.

3.4.4. Institutional issues

Seams issues can include a lack of price and operations transparency across seams (where service territories interconnect), price divergence at the seams, the difficulty of arranging interregional transmission projects, and allocating the costs of such projects.[87, 88] In turn, these issues can introduce physical vulnerabilities in terms of non-compatible control systems and procedures, decreased awareness of certain regional operations and threat or reliability issues, and disagreements about the prioritization of different mitigation strategies.

The feasibility of making changes and improvements is often a consideration when developing standards, best practice guides, and other guidance. If expectations are set too low in order to make them feasible across the entire industry, then some vulnerabilities may not be addressed by utilities that are able to do so. If the expectations are set too high, some utilities may do little or nothing, as they do not believe that they can afford to comply, rather than identifying the most cost-effective solutions for their resources. Expectations can also influence what improvements are recognized in rate cases.

Another category of institutional issues relates to barriers posed by restrictions on information sharing and specific regulatory situations. These may increase vulnerabilities if appropriate actions cannot be taken in time. Some of these restrictions are illustrated by the situation with gas generation:

- Historically, there was information sharing between the gas and electric industries, particularly on a regional basis. With deregulation, most operational information has become business confidential and proprietary, leading to difficulties in coordination.[89] Recently, the Federal Energy Regulatory Commission (FERC) has tried to take steps to open communications in order to improve reliability.
- Limitations on fuel switching at generation plants is another concern, and increased ability to switch from gas to oil without violating state or federal regulations would reduce the vulnerability to fluctuations in the gas supply.[90]

Information sharing is difficult, in part, due to issues with the electric sector owners and operators having sufficient clearances in order to receive certain threat information *and* the secure locations necessary to exchange that information in real time when there is a threat indicator. One of the ongoing issues for critical infrastructure owners and operators is obtaining actionable threat information, which is often not available as the threat indicators may not be that specific. The information-sharing councils and organizations described in Section 7 are intended to facilitate greater two-way information sharing.

3.5. Mitigation and Protection

While threats to and vulnerabilities of the electric grid exist, they can be mitigated or managed to help minimize the overall risk to the grid. A number of nationwide structures have been established to help manage risk and increase security and resilience.

The National Infrastructure Protection Plan (NIPP) 2013 mentions several approaches to managing risks. Ideally, individual decisions should be based on the importance of the affected infrastructure, the cost of the mitigation measure(s), and the expected amount of risk reduction resulting from implementing the measure(s). The groupings included in NIPP 2013 are:[91]

- Identify, deter, detect, disrupt, and prepare for threats and hazards
- Reduce vulnerabilities
- Mitigate consequences

PPD-8 – National Preparedness "is aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber attacks, pandemics, and catastrophic natural disasters."[92] PPD-8 addresses five mission areas: prevention, protection, mitigation, response, and recovery. Several policy documents, such as the National Planning Frameworks, were created under PPD-8. One of the frameworks is the National Protection Framework.[93]

The National Protection Framework focuses on core capabilities that are applicable during both normal day-to-day operations and augmented operations that take place during periods of heightened alert, incident response, or planned events in which additional or enhanced protection activities are needed. For critical infrastructure protection, this includes actions to deter the threat, reduce vulnerabilities, or minimize the consequences associated with a terrorist attack, natural disaster, or human-caused disaster on the physical and cyber elements of critical infrastructure. Specific capabilities in the protection area include Intelligence and Information Sharing; Interdiction and Disruption; Screening, Search, and Detection; Access Control and Identity Verification; Cybersecurity; Physical Protective Measures; Risk Management for Protection Programs and Activities; and Supply Chain Integrity and Security.[94]

3.5.1. Intelligence

It is not possible to protect against all events, so there needs to be a rationalization of what can and should be protected. To best address the threats and vulnerabilities facing the electric grid, there must be relevant and actionable information about those threats so that appropriate protection measures can be implemented. This can come in the form of developing intelligence from the National Intelligence Community about a specific threat (threat indicators), typically passing through DOE and DHS as part of that community, or the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS) in Canada, or through other channels, such as local or state/provincial law enforcement.

However, another critical type of intelligence deals with advance information on:

- Size and nature of attacks that are possible (from the Intelligence Community and researchers);
- Likely damage that such attacks could cause to elements of the grid (based on testing, research, and international experience);
- Expected primary, secondary, and tertiary impacts of a successful attack on parts of the grid (i.e., cascading events) (based on testing, analysis, and international experience); and
- Relative likelihood or level of concern about different types of physical attacks (from threat, vulnerability, or risk assessments, coupled with assessments of capabilities and motives).

The last of these is difficult to obtain in an unclassified form, but any guidance that can be offered in this area can greatly assist in the prioritization of efforts to protect the grid and mitigate the consequences of an attack. All of these are useful in protection and mitigation planning.

One key area of study by DOE, the national laboratories, industry and its associations, and other federal agencies is increasing the understanding of interdependencies. This can be addressed analytically, through observations of the impacts of events that occur regardless of cause (i.e., technological failure, human error, natural hazard, or attack) and through greater cross-sector sharing of information on critical systems and assets, as well as their functions and services.

3.5.2. Risk mitigation and protection measures

The electric industry has a defense-in-depth, layered approach to grid security. Recent testimony from EEI noted that "… the industry is subject to rigorous, mandatory, and enforceable reliability regulations; closely coordinates with industry and government partners at all levels; and has efforts in place to prepare, respond, and recover should power grid operations be impacted."[95]

Examples of a number of activities related to physical threats and vulnerabilities under the three layers of the defense-in-depth approach cited above:

- **Security standards and regulations.** Industry is implementing new mandatory physical security requirements under NERC's regulatory standards.[96]
- **Close coordination and sharing of threat information.** On the physical security side, the sector's ESCC is working closely with the government to understand the EMP threat. One such project is being undertaken by the Electric Power Research Institute (EPRI) to enhance our understanding of system impacts should such an attack occur and to explore the effectiveness of mitigation strategies (including hardening and recovery). The project will allow grid-specific research to inform the application of technologies that will increase grid resilience and accelerate recovery.[97]
- **Planning to respond and recover.** Spares and shared equipment, as well as regular sector and multi-sector exercises, are critical to improving response and

recovery times.[98] Some of these "spare and share" programs are outlined below. Additional information on response and recovery appears in Section 6.

Some of the other risk mitigation and protection strategies underway in the electric grid are described below.

Improved Technologies and System Configurations

Some of the available measures relate to changing the actual vulnerabilities of the equipment, while others are to deter or disrupt hazards or reduce potential impacts.

- To mitigate the impacts of damage to LPTs, there are a number of efforts underway (see the coordinated assistance program described below) to streamline the different types of transformers deployed across one utility, let alone different utilities, if existing transformers can be replaced (on their natural replacement cycle) with transformers that have more interchangeability across the utility's service territory, then it is easier to stock a few spares that can be used anywhere in the territory with the same rating, thus speeding up recovery efforts. Manufacturing, transportation, and installation of replacement transformers also are simplified.[99] At the same time, interchangeable components and interoperable systems reduce the inherent benefits of diversity, where not all equipment/systems have the exact same vulnerabilities.

  EPRI and DHS recommended that industry work with transformer manufacturers to first specify more broadly applicable spares, and then move to replacement transformers. The goal would be to first work within a utility and then within a region.[100] However, if the ultimate goal is to create greater interchangeability within a region, early communications about that goal would create greater unity of effort across the utilities.

  NIPP 2013 also promotes risk management and mitigation through infrastructure and control system design. When security and resilience issues are considered in designs from the beginning, it is easier and more cost effective to incorporate the necessary measures to mitigate physical and cyber vulnerabilities.[101]

  Some of the more traditional protective measures for LPTs also help protect against theft and improve public safety,[102] and have applicability to other equipment on the grid:

  - *Protecting information about critical substations, generating plants, and control centers.* These might include engineering drawings, site security information, modeling results, and other information useful for identifying vulnerabilities.
  - *Monitoring and detecting threats and operating conditions.* This may include the deployment of video cameras, motion detectors, thermal imaging, acoustical monitors, aerial drone surveillance of remote sites, and periodic inspection by security employees.
  - *Restricting physical access.* This can include segregating a facility into specific zones with associated access restrictions (e.g., locks, card readers) for employees and contractors, using physical barriers and controls for vehicle entry and inspection, and having full-time guards where necessary.
  - *Deploying barriers.* In addition to restricting access, visual barriers such as opaque or hardened fencing, tall fences, and protective walls limit the potential for visual data collection and the execution of a physical attack.

  - Modifying facility designs to make them more resistant to physical damage. This might mean hardening some of the surrounding equipment.
  - *Reconfiguring facility layouts or refining site selection criteria.* This could mean changing the position of equipment to shield more vulnerable components, reducing external sight lines, or creating internal or external buffer zones to limit the spread of fires or the effects of explosions.
- To help address specific gas supply vulnerabilities, additional equipment at the gas generation facilities can mitigate the impacts of a partial interruption of gas supply. Specifically, if pipeline pressure cannot be maintained at normal levels, than onsite booster compression could compensate for the loss in line pressure and help maintain the necessary burner-tip pressure to keep the units from tripping out.[103]
- Other technological changes might include enhanced duel-fuel capabilities and additional storage options, but these must be accompanied by operational preparedness to make the switch and the necessary permissions to burn oil as state, federal, and provincial environmental regulations limit the amount of oil that can be burned.[104]
- DOE works collaboratively with the DHS Science and Technology Directorate (S&T), other federal agencies, electric asset owners and operators, trade organizations, vendors, national laboratories, universities, and research organizations to advance technology. Specific areas of work with which the energy sector is looking for support include expanding on existing work in "monitoring and analysis of geomagnetically-induced currents, the impact of GMD [geomagnetic disturbance], EMP, and other physical threats on critical grid components including LPTs and bushings."[105]
- Natural Resources Canada (NRCan) works with its partner agencies, universities, and industry to perform all-hazards threat research and technology development to enhance the security and resilience of the electricity grid. Activities include research, site assessments, technology testing, and compliance analysis. Specific areas of engagement include smart grid technology, malware, and uninhabited aerial vehicles.
- DOE and the national laboratories regularly conduct analyses and studies to enhance the state of knowledge of the sector and offer approaches to mitigation and protection. Some of the recent and current work covers the following areas:
  - Grid Modernization Laboratory Consortium, including several resilience and security projects (http://energy.gov/DOE-grid-modernization-laboratory-consortium-gmlc-awards)
  - Cyber and physical threats under a DER paradigm shift
  - Cybersecurity of physical electricity assets
  - Mitigating the risks of losing multiple LPTs
  - Physical security capability maturity model
  - Cyber-physical modeling and simulation for situational awareness

Coordinated Assistance Programs

Some mitigation approaches involve identifying additional resources in advance that can supply equipment or personnel after an event. For instance, RMAGs are voluntary partnerships of investor-owned utilities across the United States that can offer assistance in restoring power when they are not affected, typically within their own

region. Mutual assistance efforts can also be scaled up to address national-level outage incidents. Similar programs support municipal utilities and electric cooperatives.[106]

There are also a number of programs to increase the availability of LPTs, given the long lead times to manufacture such equipment. Some are private sector business endeavors that will stockpile spares in strategic locations (e.g., Grid Assurance™).[107] Another approach involves a spare equipment database that allows entities needing long lead time equipment to contact other entities with spares that may be available.[108]

The Spare Transformer Equipment Program (STEP) was designed to increase the industry's inventory of spare transformers, as well as the ability to quickly transfer that inventory to an area impacted by a terrorist attack. This program is based on individual companies maintaining a specific number of transformers (acquiring them if they do not currently have them). Currently, 56 utilities in the United States are members. To address the need for other transmission and generation equipment and parts, SpareConnect offers a complementary mechanism for bulk power system asset owners and operators to network with other SpareConnect participants concerning the possible sharing of transmission and generation step-up transformers and related equipment during an emergency. While STEP imposes mandatory commitments on its members to sell their spare transformers to member utilities in need, SpareConnect is a referral service without such an obligation to provide the equipment.[109]

Workforce Training

In addition to ensuring that critical corporate knowledge (on operations, emergency procedures, reporting, etc.) is captured and transferred from one employee to another, the entire workforce must understand that they need to observe security measures. These include: (1) not providing access to others, (2) maintaining possession of identification badges, (3) keeping passwords and access codes secure, (4) protecting laptops and other electronic equipment with company data on them, (5) protecting reports and drawings, (6) not discussing company information with others, (7) not providing unauthorized tours of the facilities, (8) completing all security training, (9) not leaving ladders and other means of access along fence lines, and (10) ensuring that any vehicles brought onsite are not compromised.

They should also be trained to be observant of online and telephone phishing scams, suspicious activity around the facility (e.g., parked cars, persons with binoculars, drones), or questionable employee behavior. Some of the motivators for insider threats can come from a desire to revenge a perceived wrong, radicalization to advance religious or ideological objectives, or a willingness to seek illegal means to financial gains.[110] Other employees may be able to detect some of these behaviors or suspect that a new employee has ulterior motives.

On a more job-specific basis, all employees can be trained to identify vulnerabilities in procedures, design, or maintenance activities. This is particularly important as more integrated cyber-physical systems are installed.

Application of Risk Assessment Methodologies and Tools to Prioritize Mitigation Strategies

Risk assessment methods continue to evolve to meet particular needs and available data. When dealing with physical threats, the lack of data on the likelihood of different threats is a real challenge, and it drives the need to gain long-term intelligence, not just information on threat indicators. Threat assessments can be a critical part of this. This will further government and industry's ability to assess and prioritize risks to inform protection activities and the selection of mitigation strategies.

Tools such as the Interruption Cost Estimate (ICE) Calculator help reliability planners at utilities, government organizations, or other entities to estimate interruption costs and/or the benefits associated with reliability improvements (http://www.icecalculator.com), assisting in the selection of mitigation strategies.

Assessments of both dependencies and interdependencies are also critical to understanding risks and making risk management decisions. Such assessments are important on both sector-wide and facility-specific bases. As equipment changes, advanced control systems are implemented, generation sources change, and critical customers are added, such assessments must be updated. The Energy Sector-Specific Plan identified the need for a comprehensive framework for interdependency modeling and simulation, building on tools already available for individual infrastructure.[111]

3.6. Current and Future Trends Impacting Grid Security

Numerous current and future trends have been discussed throughout this section that may negatively or positively (or both) impact physical threats and vulnerabilities. Key items appear in Table 2.

Table 2: Future Trends and Their Likely Impacts on Physical Security

Trend	Likely Impact
Increased reliance on ICT	More precise operations and less significant outages, but increased vulnerabilities may be introduced on the cyber side
More reliance and use of smaller solid-state electronics that use less energy	Increased vulnerability to nuclear EMP and non-nuclear directed energy weapons
Increased integration of physical and cyber systems	Potentially increased vulnerabilities and consequences as cyber attacks can impact physical systems
Increased use of third-party equipment and services	Increased requirements for access by third parties requires controls to ensure that new threats are not introduced
Increased natural gas generation and coal retirements	Increased interdependence between electricity and natural gas, plus supply chain risks because natural gas for electricity generation does not involve onsite storage/reserves

Trend	Likely Impact
Increased incorporation of DER, including storage and renewable resources	Requires more grid coordination and the necessary technological and operational changes can introduce vulnerabilities, but may improve restoration times after an event; also increases the number of potential targets that may not have the same physical security as large generation plants
Current and future deregulation challenges, particularly on information sharing	Enhanced coordination and understanding of interdependencies between gas and electric at a detailed level
Changes in demand on a regional level with demographic changes and associated geographic shifts	Uncertain
Increased standardization and flexibility of critical components	Potential for reduced impacts of physical attacks due to more efficient replacement and restoration; however, the ease of impacting multiple pieces of equipment in one attack may increase as all components share the same vulnerabilities
Coordinated assistance programs	Use of industry assistance programs, such as for LPT spares, helps reduce the consequences from transformer loss/downtime
Investment challenges	Competing demands for new technology adaptation and replacement of aging infrastructure may leave the grid more fragile
Increased recognition of the value of security by financial markets and regulators	More incentive for industry to make improvements addressing physical security
Increased interdependencies with other critical infrastructure	Additional sources of threats and vulnerabilities

4. Cyber Threats and Vulnerabilities

The North American power grid is evolving to take advantage of new capabilities with ICT to increase the reliability and efficiency of the electric system. However the increased use of ICT can introduce new vulnerabilities, so cybersecurity must equally evolve. The U.S./Canadian power grid has become a valid target for attackers from a multitude of originators. Consequently, cybersecurity to protect the grid must continue to increase in sophistication.

4.1. Cyber Threats

The connectivity of the energy grid now extends directly into the homes and businesses of customers. This ever-expanding connectivity brings the grid to the customer in an effort to improve energy efficiency, but it also has the byproduct of extending the grid's attack perimeter well beyond the physical protection of the corporate environment. An adversary may now plan an attack, perform the necessary cyber reconnaissance and espionage, and execute the attack all from the privacy and safety of his or her home, whether residing in the United States or in some foreign land.

However, while network breaches tend to garner the news, the threat to the energy grid is much broader than simply protecting a network from a security breach. The Information Systems Audit and Control Association (ISACA) identifies the following types of malicious cyber-related activities:[112]

- Hacking
- Malicious code
- Loss of intellectual property
- Phishing
- Denial of service
- Insider damage

Securing the energy grid may seem as straightforward as properly controlling access to the grid; however, it is the entire set of malicious activities identified above that must be acknowledged and protected against.

Furthermore, an attack may not, and often is not, an all-out breach of a system. Cyber espionage can take the form of cyber surveillance. An adversary will gain unauthorized access and monitor network or user activity undetected to gain additional information. It could be the information itself that is the target of the breach, or the adversary may be gathering information that can be used for an all-out future attack. That a breach has not been identified does not mean that an attack is not already underway.

4.1.1. Sources of threats

Having an understanding of the threats and motivations of cyber attackers is useful to design and implement cybersecurity countermeasures. Motivations vary widely across

the spectrum of adversaries, so it is helpful to understand how each type of adversary may implement a cyber attack.

State and Non-state Actors

With its contributions to recent foreign conflicts, the United States has demonstrated dominance in conventional warfare. With this demonstration, the United States has also demonstrated its extensive reliance on computers and computerization. With a heavily computerized society, and its corresponding reliance on electricity for the execution of both defensive and offensive actions, we can expect that adversaries of the United States will attempt to take advantage of this reliance. The connectivity of the modern power grid provides adversaries not only with a new avenue by which to attack the power grid, but also with the convenience of attacking it from the safety of their home soil. A cyber attack on the power grid is an offensive maneuver that must be anticipated as part of modern, hybrid, state warfare. Countries possess the funding and resources to execute a sophisticated attack. Intelligence agencies and militaries around the world are preparing offensive weapons to be at the ready in the event of a conflict, with these actions intended to sustain a long-term campaign of attacks.[113] However, state actors are not the only entity capable of launching a sophisticated attack.

Terrorists or radicalized extremist groups will soon have, or may already possess, the knowledge necessary to execute an attack on the power grid.[114] This class of actors may also be well funded and possess the resources required to launch a sophisticated attack.[115] In addition, the concept of "hack for hire" exists when the finances are available but the resources are not.[116]

While the most serious attacks will likely be tactical in nature, the most basic hacking attempts today are strategic, focused cyber espionage aimed at the theft of sensitive, confidential, and proprietary data.[117] The originators of these types of attacks may be state or non-state actors. State actors will be incentivized to give the country an advantage; non-state actors could be looking for a corporate competitive advantage.

Finally, cyber criminals may act for notoriety or for financial gain as evidenced by the increasing rate of ransomware attacks. A Michigan utility recently became the first publicly reported victim of a ransomware attack against a public utility in the United States.[118]

Insider Threats

While external cyber attacks garner the news, insider threats actually may be the greater risk.

"Despite the attention that hackers and other external security threats receive, it is internal, not external threats, which may be the greater risk."[119]

The insider threat is not normally considered a cyber attack. One dimension of the insider threat may be realized when access to information is not properly managed, and the insider is able to access information to which he or she does not have a true "need to know." While it is not possible to completely remove the risk of a rogue employee divulging information to which he or she has legitimate access, proper provisioning of accounts and segmentation of data enable better access control decisions. The use of a

physical token for system access mitigates the potential for an unintentional release of an access password by an unsuspecting individual.

Furthermore, "the potential for combined physical-cyber attacks where an insider is involved must also be considered."[120] "… [A] coordinated attack that combined and leveraged an insider attack with an external attack would carry the potential for multiplier effects and far greater consequences than a simple one-dimensional attack."[121]

4.1.2. Trends for cyber threats

Threats Increasing in Sophistication

A Pew study found that the majority of internet experts believe that cybersecurity threats are likely to increase in the coming years.[122] The size of the community of adversaries and malicious actors continues to grow as state and non-state actors identify critical infrastructure as the target of a new method of warfare, and as more information on vulnerabilities and attacks becomes easier to acquire. Newer search engines, such as the Sentient Hyper-Optimized Data Access Network (SHODAN) and Every Routable IP Project (ERIPP), make it possible to specifically find SCADA systems that are connected to the Internet.[123] Automated exploit toolkits, such as the Metasploit Framework, make it easier for attackers to target ICS.[124] Although the framework was designed as a tool to automate penetration testing, attackers use the framework for exploitation by simply replacing the payload with a malicious one.[125]

IT threat tools, such as viruses, rootkits (malicious software that enables unauthorized access while also subverting applications intended to find it), and logic bombs (malicious code intentionally inserted into software designed to execute when a specific condition is satisfied), are becoming more commonly available and accessible, as well as easier and less technical to apply at a relatively low cost to the user.[126] It is even possible to find companies selling zero-day vulnerabilities and exploits that take advantage of these. For example, ReVuln, a company based in Malta, specializes in selling zero-day vulnerabilities—newly discovered vulnerabilities that have not yet been addressed by the vendor—for SCADA systems.[127] GLEG, Ltd. Is a Moscow-based firm which sells exploits such as SCADA+ Pack, which attempts to collect all SCADA vulnerabilities into a single exploit pack.[128]

Finally, the malware worm Stuxnet, although apparently targeting an adversary control system, once discovered and revealed now enables lesser skilled hackers to incorporate its advanced techniques into their own malware for their own purposes.[129]

Threat Channels

By definition, remote access provides a means to connect to a network from a location beyond the networked facility. While this access adds convenience to business and maintenance operations, it also provides a means for someone outside of the facility to access the network if it is not secured properly. The attack on the power grid in Ukraine in December 2015 was executed through remote access.[130] Furthermore, new smart grid devices create a potential path for cyber threats by extending connectivity directly into the homes and businesses of customers.

As technology has become more portable, so have the tools available to the malicious insider. Malicious code can infect a computer connected to the Internet, which then serves as the source of data stored on a miniaturized computing or storage device, which may then be connected to a device on the air-gapped network.[131] When a USB drive or other removable storage device is plugged into a computer on a network, if the device contains malware, it can spread across the network on which the computer is attached.[132] This was the most likely route by which the Stuxnet worm infected the Iranian nuclear facilities at Natanz and Bushehr, both of which implemented air-gapped networks.[133] Exploit tools, such as Trojans and rootkits, are increasingly stealthy, which elevates the difficulty of detection and remediation.[134]

NERC Standard CIP-010-2 is intended to control the vulnerability of these devices to such threats. The purpose of CIP-010-2 Requirement 4 (Transient Cyber Assets and Removable Media) is to manage the use of removable media and other devices not connected to the network all the time (transient assets), and mitigate any potential risks their use or misuse might introduce. CIP-010-2 requires documented plans and evidence of implementation of those plans, which must address the management and authorization of transient assets, and identify methods to mitigate the risks of using these devices.[135]

4.2. Vulnerabilities

4.2.1. Critical assets

Supervisory Control and Data Acquisition / Industrial Control Systems

Having been designed in the 1960s, 1970s, and 1980s, when the idea that a malicious actor would try to attack them was inconceivable, many ICS and their protocols lack basic security measures such as authentication and encryption, making them "insecure by design."[136]

An important and often underappreciated aspect of cyber risk is that assets controlled by a communicating intelligent device are themselves made vulnerable to damage or destruction.[137] Idaho National Engineering Laboratory ran a test—Aurora—which demonstrated the potential for remote control, misuse, and damage to a small generator.[138] An analysis of the results of Aurora notes that the test demonstrated the need for comprehensive cyber and physical generator protection,[139] and goes on to identify methods to mitigate the vulnerabilities identified during the Aurora test using physical protection schemes.[140] While the first line of defense is proper network security, appropriate protection schemes should also be implemented to mitigate the vulnerabilities indicated by the Aurora test.[141]

The potential also exists for common mode failures of assets, meaning that a single exploitation of a vulnerability can be propagated across a cyber or power system network and potentially affect an entire class of assets at one time.[142] While current system design practices do provide a measure of protection from such a threat, this potential essentially redefines "single points of failure" from a system planner's perspective, distributing the effects of a single attack across an entire system or

network.[143] This may be especially relevant to many of the renewable energy systems, such as solar, where hundreds of thousands of nearly identical systems remotely connected could be influenced by a common vulnerability.

Computer patching has been long known as a necessary component of proper cybersecurity. However, critical infrastructure often operates in a unique environment that makes system patching difficult. The vulnerabilities given below were discussed for software patching at a nuclear plant, but are generally applicable to all electricity generation systems:[144]

- "The unique characteristics of industrial environments like nuclear facilities mean that even patching a facility's commercial network could have significant consequences."[145]
- "Even if a patch has been approved for software that runs on a vendor's equipment, this does not necessarily guarantee that it is safe to install."[146]
- "The mere presence of one additional piece of software, such as a plug-in, running on a system in a nuclear facility can create an incompatibility with the patch and break the system."[147]
- "The vendor will have tested that the patch is safe in several standard cases, but cannot possibly test every combination of software that a nuclear facility might be running."[148]
- "Since patching changes the configuration of a system, in a nuclear plant it also makes it harder to monitor the system for unusual behavior that might indicate infection by malware."[149]
- "It seems, therefore, that each nuclear facility must carefully assess the advantages and disadvantages of patching in each instance. Many appear to have decided that the risks outweigh the benefits and choose not to patch."[150]

NERC Standard CIP-007 requires a patch management process for tracking, evaluating, and installing cyber security patches, and requires that evidence be presented to demonstrate implementation.[151]

Remote Access as a Vulnerability

Perhaps the most pertinent example of potential vulnerabilities introduced through remote access was the attack on the power grid in Ukraine in December 2015. The attack began well before there were any observable signs of an attack, when the attackers acquired credentials using spear-phishing tactics.[152] Using legitimate credentials, the attackers were able to access SCADA systems remotely through a virtual private network (VPN), achieving remote operations control, installing destructive malware to delay recovery efforts, and uploading illegitimate firmware to remotely upgradeable network devices.[153]

The next tactic was to overwhelm the call center, thereby achieving a denial of service. However, not only did this tactic affect customers, but it also prevented internal reporting and intercompany collaboration. This distributed denial of service attack highlights the susceptibility of voice over IP (VoIP) telephony to cyber attack. In general, the most common VoIP attack is a User Datagram Protocol flood attack; as a countermeasure, network traffic should be monitored continuously to measure VoIP quality of service.[154]

While this event was unfortunate for Ukraine, it did identify operational deficiencies and, thus, lessons learned:[155]

- Spear phishing element—Needs: Awareness and phishing training, filter incoming email, and isolate the data available to control workstations (e.g., restricted email access).
- Remote access element—Needs: Connection must be highly controlled, managed, and configured.
- Control element—Needs: Better application security and logic for confirmation of actions; communication paths must be encrypted.
- Tools and technical element—Needs: Filter calls by source (call center), install the ability to disable remote management, disable remote firmware updates, maintain undefeatable backup power, and plan secondary communications channel.

NIST provides guidance for managing and controlling remote access and identifies policies and procedures for common governance, risk, and compliance of access control.[156] Additionally, NIST conveys unique technical requirements for authorizing, monitoring, and managing all methods of remote access to the smart grid information system.[157]

Information and Communications Technologies

ICT provides an effective way to cut costs, launch new business ventures, and improve efficiency. Recent studies have suggested that the use of ICT applications has the potential to reduce our nation's total energy use by 12 to 22 percent by 2020.[158] However, it is this ICT that introduces a new security risk that spans the entire spectrum of networked controls and communications. Establishing and then actively maintaining the secure configuration of ICT systems should be seen as a key security control.

By putting in place corporate policies and processes to develop secure baseline builds and to manage the configuration and the ongoing functionality of all ICT, organizations can greatly improve the security of their ICT systems. Organizations that fail to produce and implement corporate security policies that manage the secure configuration and patching of their ICT systems are subject to the following risks:[159]

- Unauthorized changes to the system: An attacker could make unauthorized changes to ICT systems or information, compromising confidentiality, availability, and integrity.
- Exploitation of unpatched vulnerabilities: New patches are released almost daily and the timely application of security patches is critical to preserving the confidentiality, integrity, and availability of ICT systems. Attackers will attempt to exploit unpatched systems to provide themselves with unauthorized access to system resources and information. Many successful attacks are enabled by exploiting a vulnerability for which a patch had been issued prior to the attack taking place.
- Exploitation of insecure system configurations: An attacker could exploit a system that has not been locked down or hardened by:
  - Gaining unauthorized access to information assets or importing malware.

- Exploiting unnecessary functionality that has not been removed or disabled to conduct attacks and gain unauthorized access to systems, services, resources, and information.
- Connecting unauthorized equipment to exfiltrate information or introduce malware.
- Creating a back door to use in the future for malicious purposes.

Industry Data on Vulnerabilities

While security hacks and network intrusions are certainly newsworthy, very little actual numeric data is available publicly that originates from corporate sources within the industry. However, security experts from outside the industry readily scour the critical infrastructure for vulnerabilities. Whether for the purpose of personal notoriety, company marketing, or simple civic duty, these security experts usually take their findings to the proper authorities before publicizing their results in the media.

However, while the availability of numeric data is very limited, an immense volume of information identifying the vulnerabilities of critical infrastructure, including the energy grid, is easily obtainable from other sources. Seemingly endless information is available via the Internet, in books, and in videos, partially demonstrated by the long list of endnotes in Appendix C.

New Vulnerabilities—Intelligent Grids

Perhaps the most significant technological changes in the energy sector can be attributed to the Smart Grid Investment Grant (SGIG) program, which aimed to accelerate the modernization of the nation's electric transmission and distribution systems.

> "Fueled by stimulus funding in the American Recovery and Reinvestment Act of 2009, electric utilities have accelerated their deployment of smart meters to millions of homes across the United States with help from DOE's Smart Grid Investment Grant program. As the meters multiply, so do issues concerning the privacy and security of the data collected by the new technology. This advanced metering infrastructure (AMI) promises to increase energy efficiency, bolster electric power grid reliability, and facilitate demand response, among other benefits. However, to fulfill these ends, smart meters must record near real-time data on consumer electricity usage and transmit the data to utilities over great distances via communications networks that serve the smart grid."[160]

In an effort to improve cybersecurity across the sector, SGIG recipients were required to submit a Cybersecurity Plan to DOE for approval before proceeding with their respective programs. DOE conducts annual site visits with each of the projects to review activities associated with implementation of the project's cybersecurity plans.[161]

New smart grid devices create another potential path for cyber vulnerability. The mass deployment of these assets redefines the nature of the traditional protection perimeter with respect to cybersecurity by extending the network into homes and businesses. The concern is not with the attack or manipulation of a single smart meter or device—as one might imagine billing fraud—but in the potential that the device provides an access point into the greater energy management system where large areas can be manipulated. This type of exploitation was demonstrated by ioActive at the 2009 Black Hat USA

conference.[162] At this conference, cybersecurity experts identified software flaws, hardware weaknesses, and inherent security risks in the overall implementation architecture.[163]

In the future, as microgrids provide a distinct opportunity to bring new capabilities, energy cost reduction, and resiliency to a power grid through distributed intelligence and autonomy, they may also introduce new vulnerabilities.[164] For example, Vehicle-to-Grid (V2G) is the concept of supporting the electrical grid by utilizing the aggregate battery storage capability of a fleet of vehicles to transfer energy from the vehicle aggregate to the grid.[165] The exchange of data between the vehicle aggregator and the grid requires two-way communications, likely to be implemented across the Internet. As a result, electric vehicles may potentially pose a security risk to microgrids because each vehicle has the ability to connect and transmit data to the microgrid.[166]

With the potential for gathering an immense amount of data using smart technologies and with the maturation of cloud technologies, cloud technologies have become an important consideration in the overall architecture of utilities.

> "Utilities are investigating how to leverage these resources, especially as the demands on them require them to be more agile while also holding down costs. Cloud computing gives utilities the ability to quickly deploy new capability that can expand or contract as demands change."[167]

When stored "in the cloud," the data is no longer controlled by the utility. Therefore, standards and specifications must be utilized to ensure that this data is stored securely. The Federal Risk and Authorization Management Program (FedRAMP) provides a cost-effective, risk-based approach for the adoption and use of cloud services.[168]

4.2.2. Supply chains

The supply chain itself represents an important potential vulnerability. The bulk power system is dependent upon long supply chains, often with non-domestic sources and links.[169] Throughout the sector, there is increased reliance on foreign manufacturers, with critical components (such as extra-high-voltage transformers and system controls[170]) and essential spare parts manufactured abroad, and a trend toward lower overall inventory levels.[171] Reduced onsite supplies and the difficulties involved in securing replacement components present complications regarding full and seamless recovery.[172]

This is also true for digital and solid-state devices such as relays and system controls on the cybersecurity side, where the potential could exist to pre-install malicious code or vulnerability into a foreign-sourced device prior to shipping to North America.[173]

4.2.3. System configuration and within-system interdependencies

The increasing use of commercial off-the-shelf systems increases the possibility that an attacker is familiar with a system implementation, thereby making it easier to hack. Using a nuclear power generation plant as an example,

> "nuclear plants built between the 1960s and 1980s run highly customized SCADA systems. The large number of vendors meant that systems, computer languages, and proprietary protocols varied widely from plant to plant. This provided "protection by obscurity." Attacking such individualized systems is difficult: Attackers would first need to acquire specific knowledge of a SCADA system's particular characteristics, which might require insider information; then they would have to identify vulnerabilities in order to write and deliver exploits to take advantage of these. And they would have to do this for each plant they wanted to attack."[174]

Since the 1990s, facilities have been increasingly integrating their SCADA systems with computer networks built from commercial operating systems, such as Windows or Linux, manufactured by a small number of vendors.[175] This offers cost savings and greater efficiency, but the growing use of these operating systems in a large number of industries around the world means that attackers are already familiar with their vulnerabilities and previously written exploits that they can use.[176] Attackers are thus able to attack with far less effort and a much greater chance of success.[177]

Although systems are highly redundant, certain key nodes, if damaged or destroyed in a coordinated manner, would have a greater impact on system restoration than others.[178] Key loads, such as military installations and other critical infrastructure components (i.e., major natural gas hubs or telecommunications facilities), are other important elements of the system from a societal perspective that must be considered.[179] In order to build on the inherent resilience of the system with respect to a coordinated attack, these key nodes should be identified and prioritized for protection within the sector.[180]

4.2.4. Institutional issues

The level of regulatory enforcement compliance controls in the energy industry will likely continue to increase.

As a countermeasure to cyber threats, the sector is increasing regulatory enforcement and compliance controls to meet those threats:

- The U.S. Commodity Futures Trading Commission approved the National Futures Association's cybersecurity guidance that will require members to adopt and enforce policies and procedures to secure customer data and protect electronic systems.[181]
- The use of different frameworks complicates the transformation of cybersecurity programs:[182]
  - NERC continues to emphasize cybersecurity by encouraging more companies to adopt Critical Infrastructure Protection (CIP) version 5.[183]
  - NERC's CIP version 5 has expanded the scope of cyber assets that power and utility companies must monitor an estimated 1,000 percent for some utilities, which is especially challenging for small and mid-sized companies required to implement the same changes but with smaller budgets and staff than larger companies.[184]
  - On January 21, 2016, FERC issued an order approving revisions to seven the most likely to have a direct impact on the security of the electric grid include

standards and six new or modified terms, and the order was published in the *Federal Register* on January 26.[2]

Liability associated with a cybersecurity breach continues to be an institutional issue.

As does any corporate enterprise, energy companies desire to mitigate the potential liability for cybersecurity breaches. All industry participants that collect energy infrastructure data or otherwise participate in the energy sector must assess their risk profile to determine the appropriate cybersecurity compliance level and requirements. Understanding government expectations with regard to prioritization of energy assets and their associated risk is necessary for cost-effective compliance program development and implementation.[185]

Committing to the requisite investment in cybersecurity can sometimes be an issue.

Comparing the number of enterprise networks in existence against the number of reported network breaches makes the probability of such an event occurring against a given network appear to be very low. Looking blindly at the statistical probability of an occurrence makes it difficult to make the case to invest in resilience for such a low-probability event when the short-term costs appear to outweigh the longer term benefits.[186] Further complicating this, the federal government, states, provinces, municipalities, private businesses, and critical infrastructure sectors each have unique concerns, methods of evaluating risk, and operating environments.[187] Consequently, even when cybersecurity experts state with near certainty that we are not aware of all the network breaches in existence today, the impetus to invest in mitigation and preparedness may only occur following a catastrophe.[188] However, it is when a breach event actually occurs that we should investigate these situations to learn from the experiences of others, both nationally and internationally, and to initiate action by fully understanding the significant adverse impacts and costs that can be mitigated.[189]

4.3. Mitigation and Protection

4.3.1. Intelligence

Both the federal government and electric system asset owners and operators have distinct realms of responsibility and expertise in protecting the bulk power system from cyber attacks.[190] The optimal approach to utilizing the considerable knowledge of both government intelligence specialists and asset owners in ensuring the cybersecurity of the nation's electric grid is to promote a regime that clearly defines these complementary

[2] "The Federal Energy Regulatory Commission (Commission) approves seven critical infrastructure protection (CIP) Reliability Standards: CIP-003-6 (Security Management Controls), CIP-004-6 (Personnel and Training), CIP-006-6 (Physical Security of BES Cyber Systems), CIP-007-6 (Systems Security Management), CIP-009-6 (Recovery Plans for BES Cyber Systems), CIP-010-2 (Configuration Change Management and Vulnerability Assessments), and CIP-011-2 (Information Protection)." [*Source:* "Revised Critical Infrastructure Protection Reliability Standards," *Federal Register*, 2016, https://www.federalregister.gov/articles/2016/01/26/2016-01505/revised-critical-infrastructure-protection-reliability-standards.]

roles and responsibilities, and provides for ongoing consultation and sharing of information between government agencies and the electric power sector.[191]

However, the private sector can sometimes be disadvantaged in assessing the degree and urgency of possible or perceived cyber threats because of inherent limitations on its access to intelligence information.[192] The federal government is entrusted with national security responsibilities and has access to volumes of intelligence to which electric companies and other asset owners and operators are not privy.[193] On the other hand, electric utilities are experienced and knowledgeable about how to provide reliable electric service at a reasonable cost to their customers, and understand how their complex systems are designed and operate.[194] Owners, users, and operators of the electric grid are in a unique position to understand the consequences, as well as the costs, of a potential malicious act, and the benefits of proposed actions to prevent such exploitation.[195] To this end, the electricity sector has promoted cybersecurity legislation that would facilitate greater cooperation, coordination, and intelligence sharing between government and the private sector.[196] Basically, *the more actionable the threat information the government can provide, the better the sector can respond to the threat*.

Congress has been trying for years to pass cybersecurity legislation. First, the Cyber Intelligence Sharing and Protection Act (CISPA) was intended to address the needs of electric companies by providing timely and actionable information from government partners that can help protect electric companies' computer networks. Its intent was to address the legal and logistical barriers that have limited the sharing of cyber threat information between and among elements of the public and private sectors.[197] CISPA has been passed by the U.S. House of Representatives on each occasion it was introduced or reintroduced, but it has never received the approval of the U.S. Senate.

CISPA was widely criticized by advocates of Internet privacy and civil liberties with the argument that it will be used to conduct even deeper surveillance into the lives of Internet users worldwide.

In October 2015, the U.S. Senate introduced the Cybersecurity Information Sharing Act (CISA). CISA was passed by both the House and Senate, and was signed into law on December 18, 2015. CISA was designed to create a voluntary cybersecurity information-sharing process that encourages public and private sector entities to share cyber threat information while protecting classified information, intelligence sources and methods, and privacy and civil liberties. CISA requires the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of appropriate federal entities, to jointly develop and issue procedures to facilitate and promote the sharing of classified and unclassified cyber threat intelligence and defensive measures by the federal government, as well as other information and best practices related to mitigating cyber threats. The document, *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government Under the Cybersecurity Information Sharing Act of 2015*, fulfills that requirement.[198]

4.3.2. Information sharing

In February 2015, President Barack Obama released Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing, to encourage and promote sharing of

cybersecurity threat information within the private sector and between the private sector and government.[199] This Executive Order:

- Encourages the development of information-sharing and analysis organizations (ISAOs) to serve as focal points for cybersecurity information sharing and collaboration within the private sector and between the private sector and government.
- Directs DHS to fund the creation of a nonprofit organization to develop a common set of voluntary standards for ISAOs.
- Increases collaboration between ISAOs and the federal government by streamlining the mechanism for the National Cybersecurity and Communications Integration Center (NCCIC) to enter into information-sharing agreements with ISAOs.
- Adds DHS to the list of federal agencies that approve classified information-sharing arrangements and takes steps to ensure that information-sharing entities can appropriately access classified cybersecurity threat information.
- Ensures that information sharing enabled by this new framework will include strong protections for privacy and civil liberties.

Another information-sharing mechanism, the Cybersecurity Risk Information Sharing Program (CRISP), is a public-private partnership that is co-funded by DOE/OE and industry. The purpose of CRISP is to collaborate with energy sector partners to facilitate the timely bidirectional sharing of unclassified and classified threat information, and to develop situational awareness tools to enhance the sector's ability to identify, prioritize, and coordinate the protection of their critical infrastructure and key resources.[200] CRISP is a voluntary program to facilitate the exchange of detailed cybersecurity information among electric utilities, the Electric Information Sharing and Analysis Center (E-ISAC), DOE, and Pacific Northwest National Laboratory to enable electric power critical infrastructure operators to better protect their networks from sophisticated cyber threats. CRISP has two differentiators from other commercially available cyber risk monitoring services: The first is the intent and ability to integrate other cyber-related threat information provided through governmental sources with the cyber threat information gathered from the information-sharing devices installed at the participants' sites. The second is the ability of the program to look across organizations within the Electricity Subsector, identifying correlation and trends.

4.3.3. National coordination structures

PPD-21 highlights the role of the national physical and cyber coordinating centers in enabling successful critical infrastructure security and resilience outcomes.[201] The National Infrastructure Coordinating Center (NICC) and NCCIC fulfill this DHS responsibility within the critical infrastructure partnership.[202]

NICC is the watch center component of the National Protection and Programs Directorate's Office of Infrastructure Protection, the national physical critical infrastructure center designated by the Secretary of Homeland Security, and an element of the National Operations Center (NOC).[203] It is the national focal point for critical infrastructure partners to obtain 24/7 situational awareness and integrated actionable information to secure the nation's physical critical infrastructure.[204] When an incident or

event impacting critical infrastructure occurs that requires coordination between DHS and the owners and operators of critical infrastructure, NICC is the national coordination hub for supporting the security and resilience of physical critical infrastructure assets.[205] NICC collaborates with federal departments and agencies; state, local, tribal, and territorial governments; and private sector partners to monitor potential, developing, and current regional and national operations of the nation's critical infrastructure sectors.[206]

NCCIC is the lead cybersecurity and communications organization within DHS, serving as the national cyber critical infrastructure center designated by the Secretary of Homeland Security.[207] It applies analytical resources; generates shared situational awareness; and coordinates synchronized response, mitigation, and recovery efforts in the event of significant cyber or communications incidents by regularly coordinating with law enforcement, the Intelligence Community, international computer emergency response teams, domestic information sharing and analysis centers, and critical infrastructure partners to share information and collaboratively respond to incidents.[208]

Online resources include:[209]

- Homeland Security Information Network – Critical Infrastructure
- United States Computer Emergency Readiness Team (US-CERT) and ICS-CERT portal
- US-CERT.gov
- A National Cyber Awareness System, which provides timely alerts, bulletins, tips, and technical documents to those who sign up

During major incidents, NICC and NCCIC closely coordinate with the Federal Emergency Management Agency (FEMA) to ensure that overall critical infrastructure status and impacts on life and safety are understood throughout the federal incident response community.[210] Both NICC and NCCIC provide liaisons directly to the National Response Coordination Center to ensure continuous bidirectional information flow.[211]

NICC and NCCIC, as information management and coordination centers, are capable of handling information under a wide range of caveats, including, but not limited to, Classified, For Official Use Only, Personally Identifiable Information (PII), Sensitive PII, Protected Critical Infrastructure Information, Chemical-Terrorism Vulnerability Information, Law Enforcement Sensitive, and various industry standards.[212]

Additionally, chartered under the basis of HSPD-7, the ESCC fosters and facilitates the coordination of sector-wide, policy-related activities and initiatives designed to improve the reliability and resilience of the electricity sector, including physical and cybersecurity infrastructure. The ESCC is covered in more detail in Section 7.

4.3.4. Risk mitigation

Technologies and Technical Practices

In 2014, NIST released a three-volume report detailing guidance for the development of cybersecurity strategy.[213] Although this publication is focused on the smart grid, its guidance may be extended to any ICT or complex infrastructure.[214] The set of

cybersecurity requirements identified in this report is an outcome of a general high-level risk assessment performed by identifying assets, vulnerabilities, and threats and specifying impacts.[215] The report identifies an extensive set of security technologies and services to meet the set of cybersecurity requirements and mitigate the risks that are the target of these requirements.[216]

Administrative Practices

In 2012, officials from DOE, DHS, and the White House met with representatives from the major electric and nuclear sectors' trade associations to initiate this dialogue.[217] Also, a classified briefing was given to more than 70 electric company chief executive officers (CEOs) on national security threats to the industry.[218] These engagements improved CEO awareness, and resulted in the formation of a working group of CEOs, national security staff, and DOE and DHS leadership to coordinate national-level planning and preparation for response and recovery efforts before a disaster strikes.[219]

In 2012, the electric power industry collaborated on a White House initiative led by DOE, in partnership with DHS, to develop the Electric Sector Cybersecurity Capability Maturity Model (ES-C2M2) to help measure and improve the industry's cyber readiness.[220] The model helps electric utilities and grid operators to assess their cybersecurity capabilities and prioritize their investments to enhance cybersecurity.[221]

The electric power industry is closely engaged with NIAC, a public-private council that advises the President on critical infrastructure security.[222] In 2010, NIAC published *A Framework for Establishing Critical Infrastructure Resilience Goals*, which recommended executive-level dialogue between the electricity sector and government leaders.[223]

Securing Physical Cyber Assets

While the term *cyber* usually conjures the concepts of online and virtual, cyber activities are still implemented using physical assets. Proper cybersecurity must also take into account securing physical cyber assets. (Note: Use of the term *physical cyber assets* within this section is used generically and should not be confused with the proper term *BES [Bulk Electric System] Cyber Assets* as defined by NERC.)

Properly securing physical cyber assets begins by first identifying these assets. These assets include the physical hardware associated with networking and application hosting:

- Routers, hubs, switches, firewalls, etc.
- Computing platforms operating as servers, encryption devices, etc.

These assets also include ancillary support systems:

- Environmental systems such as air conditioning (especially in data centers and server rooms)
- Backup power systems such as uninterruptable power supplies
- Alarm systems

NERC has developed guidelines to identify critical cyber assets.[224]

Security Exercises

To exercise protection and mitigation measures, NERC has conducted a series of sector-wide security exercises termed Gridex. These geographically distributed exercises are designed to execute the electricity sector's crisis response to simulations of coordinated cybersecurity and physical security threats and incidents, to strengthen utilities' crisis response functions, and to provide input for lessons learned. The first grid security exercise took place in November 2011. GridEx III was the largest cyber and physical security exercise of its kind, involving more than 4,400 participants from 364 industry and government organizations in the United States, Canada, and Mexico.[225]

4.3.5. Protection

DOE has performed significant research and development within this subject area. Appendix A identifies these government actions, as well as other industry actions. One of the DOE actions was to create the Cybersecurity for Energy Delivery System (CEDS) program. CEDS was created to strengthen the energy infrastructure and protect the grid by focusing on activities such as:[226]

- Promoting best practices and investments in cyber protection.
- Sharing cyber threat data.
- Investing in cyber technologies.

Another key element of CEDS is building a culture of security, largely by making cybersecurity best practices as reflexive and common as possible, through extensive training, education, and communication.

The National Protection Framework addresses the relationship between protection and prevention.

> "As defined by PPD-8, for the purposes of the frameworks, the term *prevention* refers to preventing imminent threats from terrorism. The Prevention mission area focuses on those intelligence, technical, and law enforcement actions that prevent an adversary from carrying out an attack within the United States when the threat is imminent. Protection activities, on the other hand, focus on government and private sector measures that deter terrorist actions or deter and disrupt other threats and hazards and, like mitigation, focus on minimizing the consequences of significant events. In some cases, the same capabilities that are used for protection functions are also used in prevention operations. However, while the National Prevention Framework addresses imminent acts of terrorism, the National Protection Framework addresses all hazards and the ongoing security of potential terrorist targets. Many other activities traditionally considered preventative, such as disease prevention and cybersecurity, fall under the Protection mission area based on the distinction between Prevention and Protection in PPD-8."[227]

The Energy Policy Act of 2005 created an Electric Reliability Organization (ERO) to develop and enforce mandatory cybersecurity standards.[228] NERC was designated as the ERO in 2006, and worked with electric power industry experts to develop NERC CIP

standards CIP-002 through CIP-009, which were approved by FERC in 2008, making them mandatory for owners and operators of the bulk electric system.[229] Since 2008, the standards have been updated as the threat landscape continues to evolve.[230] The Atomic Energy Act and Nuclear Regulatory Commission also have created mandatory standards for nuclear power plants.[231]

The NERC Critical Infrastructure Protection Committee identified five steps to protect cyber assets:[232]

- Implement a security process that documents how security procedures are implemented across the utility, as well as assessment of training of personnel.
- Identify what needs to be protected in a cyber asset protection plan.
- Design for security; engineer systems with security in mind from the start.
- Operate securely; procedures and design are only as secure as the operations behind them.
- Take simple steps now, such as implementing and enforcing password policies.

To assist suppliers in managing known vulnerabilities and deliver more secure systems, DOE and DHS collaborated with industry cybersecurity and control system subject matter experts to publish *Cyber Security Procurement Language for Control Systems* in 2008. This document summarizes security principles and controls to consider when designing and procuring control system products and services (e.g., software, systems, maintenance, and networks), and provides example language that could be incorporated into procurement specifications.[233] In 2014, DOE issued procurement guidelines for building cybersecurity protections into the design and manufacturing of energy delivery systems. The *Cybersecurity Procurement Language for Energy Delivery Systems* focuses on perceived vulnerabilities in the industry's procurement process, including in software use and the account management of energy delivery systems.[234]

5. Consequences

5.1. Power Outages

The primary, national-level outcome of concern from a physical or cyber attack on the electric grid is a long-term power outage due to damage or destruction of difficult-to-replace equipment or systems. However, as soon as there is an outage, secondary and tertiary impacts start to occur. Depending on the duration, the cost of outages can include lost production and wages; loss of essential services such as transportation and water; supply chain interruptions; impacts on health care providers and other critical functions and services; public safety in times of extreme hot or cold weather; and general interruptions to all sorts of businesses and activities, including educational facilities. In addition, 99 percent of the U.S.-located Department of Defense installations rely on the grid for power.[235] The longer and more widespread the outage, the more likely that these additional impacts will be realized, underscoring the importance of understanding and managing interdependencies. Damage to the electric grid's equipment is also a concern, and can extend the duration of the outage (see Section 5.3).

Significant power outages can be caused by natural events, accidents, or deliberate attacks. While this report is focused on physical and cyber attacks, it is useful to examine historical outages to understand the impacts of such outages. The leading cause of power outages in the United States is severe weather, including blizzards, thunderstorms, and hurricanes. Severe weather accounted for 87 percent of outages affecting 50,000 or more customers from 2002–2012.[236] Studies of such events reveal the potential cost of individual extreme events. From 1980 to 2012, the United States suffered damages of $1 billion or more in 144 instances from severe weather.[237] Estimates of the annual cost of outages in the United States vary, but all range from tens to hundreds of billions of dollars, so a single extreme weather event can be a significant fraction of the annual total.[238]

The economic impacts of the August 2003 Northeast Blackout have been estimated between $4.5 and $10 billion according to three independent estimates, with DOE's estimate of about $6 billion most commonly quoted.[239] This shows the similarity to extreme weather events.

High-technology companies that produce products in batches can lose a whole day's production, even if an outage is relatively short but occurs during a production cycle—with losses in the tens of millions of dollars (if uninterruptible power supplies are not in place). The cost per hour of an outage is indicative of how quickly impacts can add up, and just how many industries rely on electricity to conduct their daily operations. The National Renewable Energy Laboratory reported a number of hourly rates in a 2003 study: brokerage operations at $6,480,000 per hour; credit card operations at $2,580,000 per hour; airline reservations at $90,000 per hour; telephone ticket sales at $72,000 per hour; and cellular communications at $41,000 per hour.[240]

5.2. Cascading Effects

Widespread blackouts with cascading effects are relatively infrequent (roughly one every seven years, on average) and each one is unique in the final sequence of events and ultimate consequences, yet they follow a basic progression as more and more areas are added to the initial blackout area. Initiating events vary and are often minor, and can include human errors, design issues, heat waves, poor vegetation management, and load/generation balance problems. The area of greatest impact may not have been proximate to the initiating event and often there were one or more opportunities to stop the progression of the failures, but human error or short-sighted procedures or decisions allowed the cascade to progress. Seven of the most significant widespread blackouts are:

- The 1965 Northeast Blackout, which impacted 30 million people in the Northeast United States and two Canadian provinces, started with a single faulty relay.[241]
- The 1977 New York City Blackout, which impacted 9 million customers, led to more than 1,000 fires, more than 2,000 stores damaged or plundered, and more than 3,500 arrests.[242, 243] The event started when two 345kV lines were struck by lightning.[244]
- The 1982 West Coast Blackout affected more than 5 million people and was initiated by a 500kV transmission tower failing in high winds and falling into a parallel tower of the same size.[245]
- The July 1996 and August 1996 Western Blackouts impacted 2 million and 7.5 million customers, respectively. Both incidents affected 14 U.S. states, 2 Canadian provinces, and Baja California. The first event was caused when a 345kV transmission line sagged into a tree and tripped out. Similarly, the second event occurred when very high temperatures in the Northwest caused two transmission lines to sag into untrimmed trees and trip out, followed by a third heavily loaded line also sagging into a tree.[246]
- The 2003 Northeast Blackout impacted 50 million people in 8 states and 1 Canadian province. The blackout in Ohio was initiated by sagging lines coming into contact with trees, and was due to deficiencies in corporate policies, lack of adherence to industry policies, and inadequate management of reactive power.[247]
- The 2011 Southwestern Blackout impacted approximately 2.5 million people in Arizona, Southern California, and Mexico's Baja California when a single 500kV transmission line initiated the event.[248]

Physically, an initial fault or short circuit causes high current/low voltage on the line containing the fault. A protective relay detects the high current/low voltage and quickly trips circuit breakers to isolate the line from the rest of the power system—all as intended. A cascade results from the sequential tripping of numerous transmission lines and generators in a widening area. Power swings and voltage fluctuations caused by the initial events can cause other lines to detect high currents/low voltages that appear to be faults, although faults may not exist on those other lines. Generators are tripped off during a cascade to protect them from severe power and voltage swings; there may not be enough power to restart once the cascade occurs, but there is no associated equipment damage affecting restoration.[249]

Cascading failures are a major concern as they are capable of escalating smaller events into large ones, like some of the ones seen in North America over the past 40 years. Cascading failures illustrate why it is important to understand interdependencies within the grid, as well as with other critical infrastructure. It also shows how critical a role advanced technology, policy, and geographical interconnectivities play.

5.3. Insufficient Reliability

A physical or cyber attack might not achieve (or even be intended to achieve) a widespread outage. In some cases, physical damage that renders equipment inoperable might reduce capacity at a generation facility or switching station, or in transmission lines. This might limit the ability to meet normal demand, or it might make that portion of the grid susceptible to more routine events, like minor storms or equipment failures. If power has to be rerouted due to inoperable equipment, the alternative paths may not have sufficient redundant capacity to handle the increase in flow needed to handle the loads from the impacted part of the grid. This can affect critical loads that rely on uninterruptible power if the new route is not sufficiently stable.

Tampering with controls through a cyber attack might affect equipment and/or lead to improper operating decisions based on faulty information, as in Ukraine. Such propagations of events mean that the initial attack can be smaller, yet still yield larger consequences. More subtle attacks might cause intermittent problems, delaying their detection.

5.4. Equipment Damage

There is a broad range of potential equipment damage resulting from an attack, depending on the nature and scale of the attack, and the skill and sophistication of the attackers:

- Cyber-generated damage such as overspeed of an electric generator's turbine, if overspeed protection can be defeated
- Cut transmission lines
- Toppled transmission towers
- Physical damage to circuit breakers
- Destruction of servers through force or fire
- Malware installed on servers and pushed to devices
- Natural gas pipeline ruptures or significant leaks
- Damaged communications systems
- Electric current-induced damage (from an EMP) to cables, transformers, electronic devices, and control systems, caused by overloading their circuits
- Direct damage to transformers caused by fires or active shooters
- Damage to industrial equipment, appliances, and personal electronic devices

5.5. Implications of Grid Disruptions and Outages

Major attacks on the grid could come from nation-states or select non-state actors, not necessarily terrorist organizations. However, the findings below indicate the potential magnitude of the consequences of a major attack:

> "A systematically designed and executed terrorist attack could cause disruptions considerably more widespread and of much longer duration than the largest power system disruptions experienced to date. Since those disruptions have entailed economic impacts approaching 10 billion dollars, it appears possible that terrorist attacks could lead to costs of hundreds of billions of dollars—that is, perhaps as much as a few percent of the U.S. gross domestic product, which is currently about $12.5 trillion. If large, extended outages were to occur during times of extreme weather, they could also result in hundreds or even thousands of deaths due to heat stress or extended exposure to extreme cold."[250]

A major attack could have a very broad range of impacts:

- Loss of a utility's proprietary data, including loss of critical performance data
- Loss of PII, including names, addresses, credit card numbers, and other information in financial records
- Inability to access critical information (such as medical records) if healthcare providers lose service
- Significant reductions in both tourism and business travel
- Loss of confidence, not just in the utility and the grid, but in the government's ability to protect the normal way of life
- Loss of access to financial accounts
- Financial losses due to production stoppage or spoilage, spoiled inventory, or lost wages. The National Academy of Science noted that a longer duration and more widespread outage than seen in past blackouts might prohibit the size of post-blackout rebound typically seen after a major outage, increasing the financial losses.[251]
- Business relocation if the geographical area is seen as a more likely target for another attack
- Ultimately loss of life and property if heating, cooling, food/water, or essential medical and emergency services (e.g., water for firefighting) cannot be provided or are compromised
- Stress on first responders and restoration crews

Physical attacks might be more localized than cyber attacks, but the propagation of problems across the grid could increase the size of the attack well beyond the initial target.

6. Response and Recovery

Emergency planning is an essential part of ensuring grid reliability because the grid is challenged by equipment failures, weather, vandalism, cyber hacks, or other events on a daily basis. Experience addressing daily aberrations helps in more severe emergencies as well, but is not sufficient for handling major response and recovery efforts. The industry has established processes for more significant events, and regularly trains and exercises employees on these practices to ensure that they are ready when needed.

PPD-8 called for the development of a National Planning System to integrate planning across all levels of government and the private sector to provide a flexible approach to prevent, protect, mitigate, respond, and recover from an event. The National Planning System includes:[252]

- National Planning Frameworks describing the key roles and responsibilities to deliver the core capabilities required for the key mission areas of prevent, protect, mitigate, respond, and recover.
- Federal Interagency Operational Plans (FIOPs) for each mission area to provide further details regarding roles and responsibilities, specify critical tasks, and identify requirements for delivering core capabilities.
- Federal department and agency operational plans to implement the FIOPs.
- Comprehensive planning guidance to support planning by local, state, tribal, and territorial governments; the private sector; and others.

FEMA is currently developing a new Power Outage Incident Annex to the Response and Recovery FIOPs, in partnership with DOE, recognizing their roles as Emergency Support Function (ESF) #12 lead agency and the Energy Sector-Specific Agency, and with the critical infrastructure Sector Coordinating Councils. The annex will address response and recovery to a widespread or long-term power outage regardless of cause. An operational draft should be released later this year and will address a significant disruption to the energy grid. Future plans are to involve states and local/regional power providers in the planning efforts. The final version of the annex will be part of FEMA's interagency consequence management system.[253]

This section presents an overview of some response and recovery structures and actions; there are too many to cover them completely.

6.1. Response

Utilities behave much like fire departments do—primarily responding to events in their own territory, but having established processes that let them provide support to other utilities in the region, or even sending crews and equipment to other regions across the United States and Canada when disasters are large enough to require such responses. Such efforts are guided by mutual assistance agreements and programs that are put in place long before they are needed, in order to avoid delays in response. If the event is associated with a severe storm, initial preparation can begin before the storm reaches an area, but for many causes of outages, including cyber and physical attacks, there is typically no warning.

For its investor-owned utility members, EEI classifies the most serious events as *national response events* (NREs). These are events that are either forecast to cause, or that have caused, widespread power outages impacting a significant population or several regions across the United States, requiring resources from multiple Regional Mutual Assistance Groups (RMAGs). There are seven RMAGs across the country. To prepare for outage events that cross RMAG boundaries, EEI and its members developed guidelines for responding to large, multi-RMAG or industry-wide NREs. When an NRE is declared, all available member emergency restoration resources can be pooled; these are then allocated to participating utilities in a "safe, efficient, transparent, and equitable manner."[254]

The American Public Power Association (APPA) formed a Mutual Aid Working Group in 2013 to establish a mutual aid network for the nation's public power utilities. More than 2,000 utilities are signatories to a mutual aid agreement that addresses coordination with federal government agencies during widespread power outages.[255] There are also mutual aid agreements to request and provide aid across both participating APPA and National Rural Electric Cooperative Association (NRECA) members. The Public Power Mutual Aid Playbook (MAP) helps ensure efficient power restoration after outages.[256]

6.1.1. Immediate identification, investigation, and action

As soon as an event occurs, the first step is an immediate investigation to identify where the problem is and what needs to be done to reroute power around the affected area. Smart meters can improve the ability of utilities to quickly and efficiently respond to power outages, unless compromised by a cyber attack. Smart meters can be used to determine the scope of an outage and to locate nested outages (commonly caused by weather events).[257] These devices also boost the efficiency of outage response teams—and, consequently, reduce utilities' operational costs—by identifying where resources are actually necessary to repair utility-side issues.

Furthermore, a report of the Executive Office of the President highlights several examples of how smart grid technologies can increase the resilience of the grid.[258] In the event of a utility grid disturbance, microgrids have the ability to seamlessly separate and isolate themselves from the rest of the grid with minimal to nonexistent disruptions to loads within the microgrid. Once utilities return to normal operations, microgrids automatically resynchronize and reconnect themselves to the utility grid in an analogously seamless manner.[259] Synchrophasor technologies are used to enhance the visibility of the transmission system. Phasor measurement units enable grid operators to more quickly identify reliability concerns and manage islanding in emergency situations.[260] Equipment health sensors can identify conditions that would lead to premature failure. By coupling these devices with data analysis tools, grid operators and maintenance personnel are provided with alerts and actionable information.[261]

The Benefits of Smart Grid Technologies

A recent example of the economic benefits of applying smart grid technologies to avoid outage costs involved EPB Electric Power in Chattanooga, TN. The utility estimated that the annual cost of power outages to the community amounted to $100 million. In an effort to reduce these costs, EPB installed automated fault isolation and service restoration technologies. Subsequently, during a July 2012 wind storm, automated switching in the distribution system instantaneously reduced the number of sustained outages by 50 percent to 40,000 customers. By coupling automated switching with data on customer outage provided by smart meters, the utility avoided 500 truck rolls and reduced total restoration time by 1.5 days. This translated into nearly $1.5 million in operational savings and substantial avoidance of costs to customers.

Source: U.S. Department of Energy and the President's Council of Economic Advisors, *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*, 2013, http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.

Additionally, advanced technologies with built-in cybersecurity capabilities are under development and deployment throughout the grid. Examples of these technologies include Padlock, a secure Ethernet data communications gateway for substations that is able to detect physical and cybersecurity tampering in field devices; SIEGate, an information exchange protocol targeted at improving cybersecurity measures for data sent over synchrophasor networks on transmission systems; and NetAPT, a software application used to help utilities map the communication paths of their control systems. These technologies can help reduce the frequency and magnitude of outages due to cyber attacks.

Among investor-owned utilities, mutual assistance agreements are activated by a member utility requesting assistance through its RMAG, or directly with other member companies in the western states. This step usually occurs as part of the response phase to prepare for the recovery phase. The RMAGs help the requesting utility identify available restoration workers and help requesting and participating utilities coordinate the logistics and personnel that will be involved in the restoration efforts. For example, RMAGs can help utilities locate specialized skill sets, equipment, or materials, and can assist in identifying other types of resources that may be needed, including line workers, damage assessors, and even call center support. EEI's mutual assistance program offers many benefits to the industry, as well as to the affected utility, including:[262]

- "Strengthens relationships among electric utilities;
- Provides a means for electric utilities to receive competent, trained employees and contractors from other experienced utilities;
- Provides a predefined mechanism to share industry resources expeditiously;
- Mitigates the risks and costs of member utilities related to major incidents;
- Proactively improves resource-sharing during emergency conditions;
- Shares best practices and technologies that help the electric power industry improve its ability to prepare for, and respond to, emergencies;
- Promotes and strengthens communication among RMAGs; and

- Enables a consistent, unified response to emergency events."

For cyber attacks, another resource is the DHS ICS-CERT, which works closely with the entire energy sector and has worked onsite to help resolve spear-phishing campaigns that seem to target ICS/SCADA data, including data that could facilitate remote access and control of systems.[263]

In addition, communications with operators of neighboring systems on the grid to share information about outages enables those other operators to help preserve the integrity of the grid.[264] In addition, communications with the public are also critical, and likewise must begin immediately to help limit misunderstandings and possible chaos. The public will use many different communications channels and will fill any voids with speculation and rumors if the best information available is not provided by the utilities.

6.1.2. Investigation

Utilities typically sponsor both internal and independent investigations of the causes of major outages and damage. For very significant events, trade associations and federal agencies (such as DHS through ICS-CERT or the FBI's investigation teams) may investigate as well. These differ from the immediate investigations that try to target what parts of the grid were affected and what damages occurred. The detailed investigations are longer term, and are intended to determine both how an individual or group was able to successfully execute an attack and to understand how the grid and its components reacted. This may allow lessons learned and best practices for protection and mitigation to be shared to help minimize both the vulnerabilities to, and consequences of, future attacks on other parts of the grid.

Determining the specifics of the attack allows utilities to know what some of the indicators of an impending attack are, and also to take the appropriate measures to try to limit the potential for future attacks through changes in procedures, physical security measures, employee screening, equipment hardening, access to control systems, passwords, and so forth. Understanding how the grid and its components reacted allows for appropriate changes in control algorithms and set points, training, operating procedures, and equipment design and configuration.

The increased understanding of the event also provides potential legal recourse for recovering costs or critical intelligence for the appropriate authorities.

6.1.3. National response efforts

Under the National Response Framework, ESF #12—Energy facilitates the reestablishment of damaged energy systems and components when activated by the Secretary of Homeland Security for incidents requiring a coordinated federal response:[265]

- "Provides technical expertise to energy asset owners and operators, other Federal agencies, and local, state, tribal, territorial, and insular area governments and conducts field assessments as needed;

- Collects, evaluates, and shares information on energy system damage and provides estimations on the effect of energy system outages within affected areas, as well as the potential regional and national impact;
- Through coordination with DOE as the primary agency, assists government and private sector stakeholders in overcoming the inherent challenges associated with reestablishment of the energy system; and
- Provides information, through coordination with DOE Headquarters, concerning the status of energy reestablishment efforts to include geographic data; projected schedules; stabilization and reestablishment tracking and completion percentages; and other information as appropriate."

When DHS/FEMA activates ESF #12 under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (hereinafter the Stafford Act), response teams are deployed as needed to affected areas to assist state, local, tribal, and territorial governments in response and restoration efforts. ESF #12 representatives, including DOE as the ESF #12 lead, also deploy to the National Response Coordination Center and the Regional Response Coordination Center.[266] The duties of DOE under ESF #12 include those shown in Table 3.

Table 3: ESF #12 Core Capabilities

ESF #12—Energy	Responsibilities
Infrastructure Systems	▪ Assist energy asset owners and operators and local, state, tribal, territorial, and insular area authorities with requests for emergency response actions as required to meet the nation's energy demands. ▪ Identify supporting resources needed to stabilize and reestablish energy systems. ▪ Assist federal departments and agencies by locating fuel for transportation, communications, emergency operations, and national defense, pursuant to the authorities available to the agency providing assistance. ▪ Through DOE, the Energy Sector-Specific Agency (SSA) addresses significant disruptions in energy supplies for any reason, whether caused by physical disruption of energy transmission and distribution systems; unexpected operational failure of such systems; acts of terrorism or sabotage; or unusual economic, international, or political events. ▪ In coordination with DOE, the Energy SSA addresses the impact that damage to an energy system in one geographic region may have on energy supplies, systems, and components in other regions relying on the same system. ▪ In consultation with energy asset owners, operators, and DOE, the Energy SSA advises local, state, tribal, territorial, and insular area authorities on priorities for energy system reestablishment, assistance, and supply during response operations.
Public and Private Services and Resources	▪ Provide subject matter expertise to the private sector as requested to assist in stabilization and reestablishment efforts. ▪ Through coordination with DOE (refer to Primary Agency Functions), ESF #12 serves as a federal point of contact with the energy industry for information sharing and requests for assistance from private and public sector owners and operators.

ESF #12—Energy	Responsibilities
Situational Assessment	▪ Work with the FEMA regions; local, state, tribal, territorial, and insular area authorities; and the private sector to develop procedures and products that improve situational awareness to effectively respond to a disruption of the energy sector. ▪ Coordinate preliminary damage assessments in the energy sector. ▪ Identify requirements to repair energy systems and monitors repair work. ▪ Through coordination with DOE, ESF #12: - Serves as a source for reporting of critical energy infrastructure damage and operating status for the energy systems within an impacted area, as well as on regional and national energy systems. - Assesses the energy impacts of the incident and provides analysis of the extent and duration of energy shortfalls. - Analyzes and models the potential impacts to the electric power, oil, natural gas, and coal infrastructures and determines the effect a disruption has on other critical infrastructure.

Source: U.S. Department of Homeland Security, *Response Federal Interagency Operational Plan*, 2014, p. A-26, http://www.fema.gov/media-library-data/1406719953589-4ab5bfa40fe82879611d945dd60230c4/Response_FIOP_FINAL_20140729.pdf.

In addition, DOE has a plethora of legal authorities that allows the Secretary of Energy to respond to emergencies outside the realm of ESF #12 or DHS/FEMA activation (see Section 7 of this report). One example is the 2003 Northeast Blackout, where DOE, based on its legal authorities, was involved in:[267]

- Coordinating with DHS and FERC in gathering information and responding to the blackout.
- Coordinating with states through its state communications program and helping them enact measures to respond to the blackout.
- Monitoring activity on the electric grid with NERC.
- Coordinating fuel status data for backup power supplies that were essential to recovery efforts.
- Tracking petroleum refinery status and shutdowns.

In Canada, the Federal Emergency Response Plan (FERP) is designed to harmonize federal emergency response efforts with those of the provinces/territorial governments, nongovernmental organizations, and the private sector. FERP applies to both domestic emergencies and to those international emergencies with a domestic impact. The plan has both national- and regional-level components, and is the all-hazards plan for a coordinated federal response to emergencies. ESF #4—Energy Production & Distribution falls under the responsibility of NRCan. It addresses "producing, refining, transporting, generating, transmitting, conserving, repairing/building, distributing, and maintaining energy systems and system components for petroleum products (oil), natural gas, and electricity. In addition, this ESF collects, evaluates, and shares information on energy system damage and estimations on the impact of energy system outages within affected areas. Additionally, ESF #4 provides information and advice concerning the energy restoration process as appropriate."[268]

The National Emergency Response System is a component of Canada's emergency response management system and applies to responses to domestic emergencies:[269]

- "Provides the linkages between the federal, provincial and territorial emergency response systems for all hazards;
- Identifies federal, provincial and territorial interactions in areas of response activities, including situational awareness, risk assessment/impact analysis, planning, logistic support coordination and public communications;
- Facilitates and expedites federal, provincial and territorial response coordination and decision making;
- Establishes standardized terminology, which can be used by federal, provincial and territorial governments and stakeholders to facilitate the timely exchange of information; and
- Describes the process for a provincial or territorial request for federal emergency assistance."

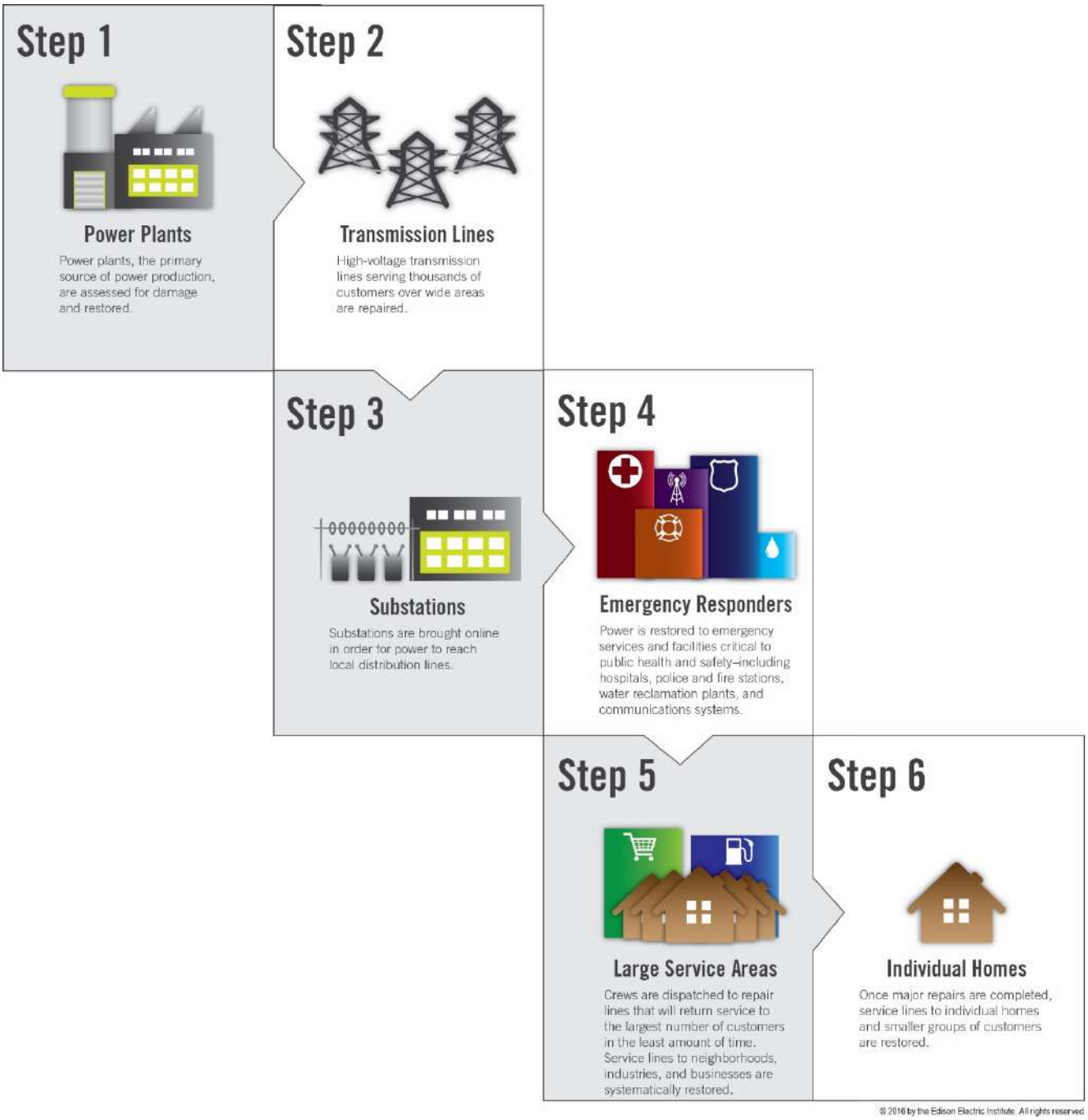
6.2. Recovery

Power restoration is enabled by established processes at each utility and across the grid. The mutual assistance programs that guide response efforts are matched by other programs to assist in restoration. Critical facilities and functions, such as hospitals and healthcare facilities, emergency services (police, fire, and emergency medical), water and water-treatment facilities, and essential transportation systems, are generally restored first, once key elements of the grid are addressed, such as power plants, transmission lines, and substations. The actual restoration sequence is determined by the utilities and the states and territories in which they operate, as well as by the specific nature of the outage, the damage incurred, and the ability to make the needed repairs.

Figure 3 illustrates a typical restoration process after a storm. Conceptually, the same basic steps apply to physical security events, although the level of damage at the community or individual home may be minimal. For cybersecurity events, the first three steps may be the most critical, depending upon the focus of the malware.

NERC's *Severe Impact Resilience: Considerations and Recommendations* (2012) outlines three restoration phases after a catastrophic cybersecurity event targeting the grid. Immediate power restoration operations would occur in the first few days. The next phase could last weeks or longer, and would reflect operations in the compromised state achievable after the attack. Only in the third phase would expected reliability and service be attained.

The Recovery FIOP provides the overall interagency coordination structure for the recovery phases of Stafford Act incidents, and the Recovery FIOP and elements of the National Disaster Recovery Framework can also be used for non-Stafford Act incidents.[270]



Reprinted with the permission of the Edison Electric Institute

Figure 3: Illustrative Restoration Process

6.2.1. Technical strategies for an efficient recovery

Available technical strategies include grid modernization, the outcomes of resilience research and development efforts for critical grid components, the hardening of assets, and maintaining secure copies of critical software.

Grid modernization, including not only advanced metering as described above, but also increased adaptation of DER, which may potentially improve grid resilience by directly serving customers during outage or power quality events, or potentially supporting restoration processes[271] and renewables to allow operation independent of a damaged grid,[272] can contribute to more rapid restoration of power after a security event. DOE's Grid Modernization Initiative is designed to improve the resilience, reliability, and security of the nation's electricity delivery system. A comprehensive new Grid Modernization Multi-Year Program Plan was released in January 2016 to set out a blueprint for DOE's efforts to enable a modernized grid.[273]

One of the suggested metrics for measuring improvements through grid modernization as noted in DOE's Grid Modernization Lab Call is "the ability of the system to operate safely and consistently in the face of all hazards. The system must be able to identify, protect, detect, respond and recover from physical and man-made situations with minimal loss of service."[274] One of the particular areas cited for research is the SCADA system and network recovery.

The Transformer Resilience and Advanced Components program includes a number of research and development activities intended to lead to improvements in the resilience of transformers. This program is intended to develop cost-effective, next-generation components that are inherently more resilient.[275]

In terms of hardening assets, a number of recent innovations are supporting the efforts by utilities:[276]

- Composite transmission poles[277]
- Infrared thermography power line inspection[278]
- Underground installation of high-temperature superconductor power transmission cables[279]
- Smart grid integration[280]
- Electric distribution recloser advances[281]

Many of these and the more traditional hardening measures are promoted due to the results of recent storms, but they can also offer benefits to protect from a number of physical and cyber threats. Placement of lines underground[282] removes the extreme visibility of overhead transmission lines, potentially reducing opportunistic physical security events.

6.2.2. Institutional strategies supporting an effective recovery

Institutional strategies include coordinated assistance programs, development of response and recovery plans and then training and exercising those plans, and increased standardization, redundancy, or flexibility of equipment.

Coordinated Assistance Programs. Damaged equipment can be repaired or replaced more quickly through coordinated assistance programs like those designed to increase the availability of long lead time equipment:

- The Spare Equipment Database System would allow entities needing long lead time equipment to contact other entities with spares that may be available.[283]
- The Spare Transformer Equipment Program (STEP) was designed to increase the industry's inventory of spare transformers and the ability to quickly transfer that inventory to areas impacted by a terrorist attack.[284]
- SpareConnect offers a mechanism for bulk power system asset owners and operators to network with other SpareConnect participants concerning the possible sharing of transmission and generation step-up transformers and related equipment during emergencies.[285]
- Grid Assurance is a business endeavor that will stockpile spares in strategic locations [http://www.gridassurance.com].[286]

A recent paper has leveraged the lessons learned from Superstorm Sandy to address restoration after a major cybersecurity event, focusing on ways to leverage existing mutual assistance agreements and other restoration mechanisms. It also identifies challenges that are unique to cyber systems (such as utility-specific ICT) that must be addressed when adapting current physically-based restoration practices, such as mutual assistance for restringing power lines and other restoration tasks.[287]

Response and Recovery Plans, Training, and Exercises. The development of response and recovery plans allows utilities to plan ahead for emergencies, and to explicitly consider not only appropriate operating procedures, but also the necessary advance logistical and resource arrangements that are needed to avoid delaying response and recovery actions. The development of similar plans on a regional basis or for one of the three interconnections within the North American grid can further ensure timely coordination when an event occurs. Such plans will be most useful if staff and appropriate local, state, and federal officials are trained on them. The training should be reinforced with drills and exercises (tabletop up to full scale) for appropriate partner groups.

Utilities can leverage exercises such as GridEx to develop specialized agreements and support protocols that can meet the challenges of a cybersecurity event, as well as for physical security events.[288]

Use of Standardized or Flexible Equipment. Standardized physical equipment and control systems and software offer a number of benefits, including an increased ability to swap parts from one installation to another, the opportunity to combine inventories of spare parts, and the ease of installation or repair when staff from one area or facility help out another location in an emergency situation. This last point can be particularly important for automated control systems.[289] Redundant equipment can also be beneficial in certain situations.

7. Roles and Responsibilities in North America

This section discusses many of the roles of different entities in helping ensure the security of the grid, including federal and state governments, owners and operators, and industry associations. It also describes some of the information-sharing and coordination structures set out in key policies and government directives.

7.1. U.S. Federal Entities

The primary federal entities within the United States with specific roles relating to security of the electric grid under normal and emergency conditions are the Departments of Energy, Homeland Security, and Justice (including the Federal Bureau of Investigation), and the Federal Energy Regulatory Commission. Many of these roles have been set forth in four key presidential documents:

- *Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience.* PPD-21 advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. The associated efforts are a shared responsibility among the federal, state, local, tribal, and territorial entities and critical infrastructure owners and operators. PPD-21 refines and clarifies the related functions, roles, and responsibilities across the federal government.[290]
- *Executive Order (EO) 12656 – Assignment of Emergency Preparedness Responsibilities.* Based on the President's authority under the U.S. Constitution and the laws of the United States, and pursuant to Reorganization Plan No. 1 of 1958 (72 Stat. 1799); the National Security Act of 1947, as amended; the Defense Production Act of 1950, as amended; and the Federal Civil Defense Act, as amended, EO 12656 sets forth the responsibilities of federal departments and agencies in national security emergencies. Many of the responsibilities apply to all agencies.[291]
- *Presidential Policy Directive 8 – National Preparedness.* This directive is aimed at strengthening security and resilience through systematic preparation for the threats that pose the greatest risk to the security of the United States, including acts of terrorism, cyber attacks, pandemics, and catastrophic natural disasters. The Secretary of Homeland Security is responsible for coordinating the domestic all-hazards preparedness efforts of all executive departments and agencies, in consultation with others, and for developing the national preparedness goal. The heads of all executive departments and agencies with roles in prevention, protection, mitigation, response, and recovery are responsible for national preparedness efforts, consistent with their statutory roles and responsibilities.[292]
- *Executive Order 13636 – Improving Critical Infrastructure Cybersecurity.* EO 13636 directs the Executive Branch to develop a technology-neutral voluntary cybersecurity framework; promote and incentivize the adoption of cybersecurity practices; increase the volume, timeliness, and quality of cyber threat information sharing; incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure; and explore the use of existing regulation to promote cybersecurity. Roles and responsibilities are set forth for federal departments and agencies in these tasks.[293]

Additional directives, orders, and acts are described throughout this section and are listed in Appendix A.

7.1.1. U.S. Department of Energy

Under EO 12656,[294] DOE is assigned a number of general emergency preparedness responsibilities along with other agencies. Part 7 sets out numerous roles and responsibilities specific to DOE, to include lead responsibilities for:[295]

- Conducting national security emergency preparedness planning and providing information on energy supply and demand conditions, and on the requirements for, and the availability of, materials and services critical to energy supply systems.
- Developing energy supply and demand strategies to ensure continued provision of the minimum essential services in national security emergencies.
- Collaboratively developing plans and capabilities for identification, analysis, damage assessment, and mitigation of hazards from nuclear weapons, materials, and devices.

Support responsibilities[296] for DOE include coordinating with the Secretary of Agriculture regarding the emergency preparedness of the rural electric supply systems throughout the United States and the assignment of emergency preparedness responsibilities to the Rural Electrification Administration.

Under PPD-21, as the Sector-Specific Agency for the energy sector, DOE serves as a day-to-day federal interface for the prioritization and coordination of sector-specific activities; carries out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations; and provides, supports, or facilitates technical assistance and consultations to identify vulnerabilities and help mitigate incidents. As the Energy Sector-Specific Plan also notes, DOE, as the Energy Sector-Specific Agency, continues to work with its partners to help identify program gaps and improve the effectiveness of infrastructure and resilience programs.[297]

The Secretary of Energy is delegated responsibilities under EO 13603, National Defense Resources Preparedness, for all forms of energy with respect to energy production and construction, distribution and use, and directly-related activities.[298] To maximize domestic energy supplies, the Secretary has the authority to make findings that materials (including equipment), services, and facilities are critical and essential.[299]

EO 13636, Improving Critical Infrastructure Cybersecurity, assigns responsibilities to the Secretary with respect to energy supply and distribution, and related activities, such as participating in the consultative process to coordinate improvements to the cybersecurity of critical infrastructure,[300] supporting the adoption of the cybersecurity framework by owners and operators,[301] and working with the sector to develop implementation guidance.[302]

Under PPD-8, the Secretary of Energy is assigned the responsibility for national preparedness efforts, including DOE-specific operational plans, as needed, consistent with DOE's statutory roles and responsibilities.[303]

Additional security-related authorities and responsibilities are assigned to the Secretary of Energy and DOE under the following:

- The DOE Organization Act of 1977[304] established DOE, in part, to develop a coordinated national energy policy. Title IV, Section 401 established the Federal Energy Regulatory Commission. The DOE Organization Act was predated by the Federal Energy Administration Act of 1974, which established the Federal Energy Emergency Administration to ensure that the nation's emergency energy needs were met for the foreseeable future and directed the Administrator to plan, direct, and conduct programs related to the production, conservation, use, and allocation of all forms of energy.[305] The Energy Supply and Environmental Coordination Act of 1974 also provided responsibilities for the concurrent interests of ensuring the energy supply and protecting the environment, including human health.[306] All of these acts addressed monitoring, collecting, assembling, evaluating, and analyzing energy information, and exercising information gathering and reporting authorities.
- 15 CFR 700, Defense Priorities and Allocations System[307] draws authority from Titles I and VII of the Defense Production Act of 1950, as amended (50 USC App. §2061 *et seq.*); Title VI of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 USC 5195 *et seq.*); and numerous Executive Orders. The resulting Defense Priorities and Allocations System includes emergency preparedness activities and critical infrastructure protection and restoration as part of the definition of national defense activities and ensures "the timely availability of industrial resources for approved programs and provides an operating system to support rapid industrial response to a national emergency."[308]
- The Federal Power Act includes the assignment of authorities when an emergency exists relating to electric energy, including the authority to order temporary connections of facilities, and generation, delivery, interchange, or transmission of electricity to address the emergency and serve the public interest.[309]
- The Fixing America's Surface Transportation (FAST) Act conveys authorities to the Secretary of Energy to enhance emergency preparedness for natural disasters.[310] It similarly provides authority to address a grid security emergency and identifies DOE as the lead Sector-Specific Agency for cybersecurity for the energy sector under an amendment to the Federal Power Act.[311] It also provides guidance on resolving environmental and grid reliability conflicts.[312] Division F, Section 61004 outlines the requirements for a Strategic Transformer Reserve Plan. Lastly, the FAST Act calls for the Secretary of Energy to establish energy security valuation methods.[313]

Collectively, these various directives, orders, and acts establish DOE's authorities and roles in planning for, mitigating, and responding to emergencies; coordinating with other agencies, various levels of government, and industry; and ensuring that the energy needs of the United States are met. Through the establishment of FERC within the structure of DOE, DOE has assurance that there are regulatory mechanisms to support its other roles, while recognizing the independence of FERC.

Federal Energy Regulatory Commission

The mission of FERC is to assist consumers in obtaining reliable, efficient, and sustainable energy services at a reasonable cost through appropriate regulatory and market means.[314] The Commission's legal authority comes from the Federal Power Act

and amendments.[315] The Office of Energy Infrastructure Security (OEIS) supports the Commission to identify, communicate, and seek solutions to potential risks to FERC-jurisdictional facilities from cyber and physical threats and attacks. OEIS also works with other agencies, national laboratories, vendors, and universities to identify effective mitigations to new threats.[316] OEIS is separated from the regulatory functions of FERC. OEIS and FERC coordinate and consult with NARUC and the state utility commissions to improve information sharing, education, and outreach efforts.

The Office of Electric Reliability (OER) helps protect and improve the reliability and security of the nation's bulk power system through effective regulatory oversight as established by Congress and the President in the Energy Policy Act of 2005.[317] This includes overseeing the development and review of mandatory reliability and security standards, and overseeing compliance with the standards by the users, owners, and operators of the bulk power system. This includes overseeing NERC's activities as an ERO (see Section 7.4.1) certified by FERC and proposing new standards where warranted. OER also monitors real-time events on the bulk power system, and operates a 24/7 emergency reporting system. FERC also regulates other critical energy infrastructure, including large hydroelectric facilities and interstate oil and gas pipelines.

7.1.2. U.S. Department of Homeland Security

Under EO 12656,[318] DHS is assigned a number of general emergency preparedness responsibilities along with other agencies. Part 17 sets out numerous roles and responsibilities specific to DHS/FEMA, to include lead responsibilities[319] for:

- Guiding and assisting government and private sector organizations in achieving preparedness.
- Coordinating the implementation of policies and programs for efficient mobilization of resources in response to national security emergencies.
- Coordinating the planning, conduct, and evaluation of national security emergency exercises.
- Providing guidance to federal departments and agencies on the appropriate use of defense production authorities, including resource claimancy, in order to improve the capability of industry and infrastructure systems to meet national security emergency needs.

Under PPD-21, the Secretary of Homeland Security is directed to provide strategic guidance, promote a national unity of effort, and coordinate the overall federal effort to promote the security and resilience of the nation's critical infrastructure.[320] Responsibilities assigned in the Homeland Security Act of 2002, as amended, include evaluating national capabilities, opportunities, and challenges in protecting critical infrastructure; analyzing the threats to, the vulnerabilities of, and the potential consequences from all hazards on critical infrastructure; and identifying and analyzing key interdependencies among critical infrastructure sectors. Numerous additional roles and responsibilities under PPD-21 focus on the identification and prioritization of critical infrastructure; providing information about emerging trends, imminent threats, and the status of incidents; information exchange; and coordinating federal government

responses to significant cyber or physical incidents affecting critical infrastructure consistent with statutory authorities.

EO 13636, Improving Critical Infrastructure Cybersecurity, assigns responsibilities to the Secretary to ensure the timely production and dissemination of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity.[321] Classified reports are to be produced and disseminated to those critical infrastructure entities authorized to receive them. Additional security clearances are to be provided, where warranted, to allow greater access to threat and vulnerability information. Additional technical information is also to be shared. Many of the other responsibilities under this order are assigned to DHS, often in collaboration with other agencies.

Under PPD-8, "the Secretary of Homeland Security is responsible for coordinating the domestic all-hazards preparedness efforts of all executive departments and agencies, in consultation with State, local, tribal, and territorial governments, nongovernmental organizations, private-sector partners, and the general public; and for developing the national preparedness goal."[322]

Whereas DOE's roles focus on energy infrastructure and its operations, security, and resilience, DHS is generally responsible for the overall frameworks, guidance, and coordination across all critical infrastructure and stakeholders in the areas of national preparedness, critical infrastructure, and cybersecurity. In the area of cybersecurity, the FAST Act[323] gave DOE unique responsibilities that, in some ways, mirror the responsibilities of DHS across the other infrastructure sectors. For designated sectors, DHS has additional responsibilities like those of DOE for energy (e.g., government facilities, chemicals, IT, communications).

7.1.3. U.S. Department of Justice

Under EO 12656,[324] the U.S. Department of Justice (DOJ) is assigned a number of general emergency preparedness responsibilities along with other agencies. Part 11 sets out numerous roles and responsibilities specific to DOJ, to include lead responsibilities[325] for:

- Providing legal advice to the President and the heads of federal departments and agencies regarding national security emergency powers, plans, and authorities.
- Developing intergovernmental and interagency law enforcement plans and counterterrorism programs to interdict and respond to terrorism incidents in the United States that may result in a national security emergency or that occur during such an emergency.

Support responsibilities for DOJ[326] include assisting in the development of plans to physically protect essential resources and facilities.

Per PPD-21, DOJ, including the FBI, shall lead counterterrorism and counterintelligence investigations and related law enforcement activities across the critical infrastructure sectors.[327] In addition, DOJ shall investigate, disrupt, prosecute, and otherwise reduce foreign intelligence, terrorist, and other threats to, and actual or attempted attacks on, or sabotage of, the nation's critical infrastructure. The FBI conducts domestic collection,

analysis, and dissemination of cyber threat information, and the sharing of information on cyber threat investigations.

Under PPD-8, the Attorney General is assigned the responsibility for national preparedness efforts, including DOJ-specific operational plans, as needed, consistent with the statutory roles and responsibilities for DOJ.[328]

7.1.4. Other U.S. Departments and Agencies

Under EO 12656,[329] the **U.S. Department of State** (DOS) is assigned a number of general emergency preparedness responsibilities along with other agencies. Part 13 sets out numerous roles and responsibilities specific to DOS, to include lead responsibilities[330] for preparing to carry out DOS responsibilities in the conduct of the foreign relations of the United States during national security emergencies, including the following:

- Formulation and implementation of foreign policy and negotiation regarding contingency and post-emergency plans, intergovernmental agreements, and arrangements with allies of the United States
- Mutual assistance activities

Under PPD-21, **DOS** shall engage foreign governments and international organizations to facilitate the overall exchange of best practices and lessons learned for promoting the security and resilience of critical infrastructure.[331]

Under PPD-21, the **U.S. Department of Commerce** collaboratively engages private sector, research, academic, and government organizations to improve security for technology and tools related to cyber-based systems, and helps enable the timely availability of industrial products, materials, and services to meet homeland security requirements.[332]

EO 13636 calls for the **Secretary of Commerce** to direct the Director of NIST to lead the development of a framework to reduce cyber risks to critical infrastructure.[333] This Cybersecurity Framework is to include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks, and incorporate voluntary consensus standards and industry best practices. It is also to be consistent with voluntary international standards, where appropriate.

Under PPD-21, the **Federal Communications Commission** partners with federal departments and agencies to identify and prioritize communications infrastructure, identify communications vulnerabilities and work with other stakeholders to address those vulnerabilities, and work with domestic and international stakeholders to increase the security and resilience of critical communications infrastructure.[334]

Under PPD-8, “the heads of all executive departments and agencies with roles in prevention, protection, mitigation, response, and recovery are responsible for national preparedness efforts, including department-specific operational plans, as needed, consistent with their statutory roles and responsibilities.”[335]

7.2. Canadian Federal Entities

Most of the electricity flows and paths in Canada flow in a north-south direction with direct interconnections between the provinces and the adjacent northern states and broader interconnections within the United States. This means that the eight provinces largely determine their policies on energy infrastructure and regulation, along with the National Energy Board (NEB). Public Safety Canada (PSC) and the other federal agencies described below play an active and important role in working with the provinces and their regulated utilities and infrastructure providers to address physical and cyber threats.

The primary federal entities within Canada with specific roles related to the security of the electric grid under normal or emergency conditions are NRCan, PSC, CSIS, Defence Research and Development Canada (DRDC), and NEB. Other government entities have important roles in emergency management and law enforcement, including the RCMP. Guiding documents include the following:

- The National Strategy for Critical Infrastructure establishes a risk-based approach for strengthening the resilience of Canada's vital assets and systems, and sets out a collaborative, federal-provincial-territorial and private sector approach built around partnerships, risk management, and information sharing and protection.[336]
- The Emergency Management Act assigns the Minister of Public Safety and Emergency Preparedness the responsibility for coordinating emergency management activities across Canada.[337] Other ministers are responsible for preparing emergency management plans related to their mandate areas, and to maintain, test, and implement those plans, as well as conduct exercises and training.[338]

7.2.1. Natural Resources Canada

Under the National Strategy for Critical Infrastructure,[339] NRCan is the designated federal lead department for the Energy and Utilities Sector. It works collaboratively with government and industry partners through the Energy and Utilities Sector Network to share information and best practices. A key initiative in these efforts was the establishment of the National Energy Infrastructure Test Centre to undertake targeted research and provide specialized training and exercises focused on the unique operating environments of the Energy and Utilities Sector.

Under the Energy Supplies Emergency Act, NRCan is provided "a means to conserve the supplies of energy within Canada during periods of national emergency caused by shortages or market disturbances affecting the national security and welfare and the economic stability of Canada,"[340] particularly for oil and gas disruptions. The Deputy Minister of Natural Resources is the Chairperson of the Energy Supplies Allocation Board.[341]

NRCan is responsible for ESF #4, Energy Production & Distribution, under the Federal Emergency Response Plan.[342]

7.2.2. Public Safety Canada

PSC coordinates the activities of all federal departments and agencies in Canada in their emergency management functions: operations, situational awareness, risk assessment, planning, logistics, and finance/administration.[343] PSC was established by the Department of Public Safety and Emergency Preparedness Act, and is overseen by the Minister of Public Safety and Emergency Preparedness.[344] PSC houses the Government Operations Centre as the hub of the overall national emergency response and incident response planning network across the provinces.

The Emergencies Act enables PSC to take temporary measures to address public order emergencies—those that arise from threats to the security of Canada and that are so serious as to be a national emergency.[345]

The Emergency Management Act recognizes the roles that all stakeholders must play in Canada's emergency management system. It sets out the leadership role and responsibilities of the Minister of Public Safety and Emergency Preparedness, including coordinating emergency management activities among government institutions and in cooperation with the provinces and other entities. The responsibilities of other federal ministers are also set out in the Act.

Canada's Cyber Security Strategy[346] falls under PSC's responsibilities and is built on three pillars:

- Securing government systems.
- Partnering to secure vital cyber systems outside the federal government.
- Helping Canadians to be secure online.

Senior-level policy coordination on cybersecurity policies for critical infrastructure occurs between PSC and the White House Office of Cybersecurity.

7.2.3. Canadian Security Intelligence Service

Overseen by the Minister of Public Safety and Emergency Preparedness, CSIS investigates and reports on activities that may pose a threat to the security of Canada. CSIS collects, analyzes, and disseminates threat-related information; CSIS can also provide security assessments to federal departments and agencies. CSIS may also take measures to reduce threats to the security of Canada in accordance with well-defined legal requirements and ministerial direction, operating within or outside of Canada.[347]

7.2.4. Royal Canadian Mounted Police

Also overseen by the Minister of Public Safety and Emergency Preparedness, the RCMP enforces Canadian laws; prevents crime; and maintains peace, order, and security.[348]

7.2.5. Defence Research and Development Canada

DRDC leads government efforts in defense and security science and technology, serving government departments and the public safety and national security communities. The Defence and Security S&T Strategy sets out six primary objectives, including three impacting grid security:[349]

- Enable the acquisition, sharing, and use of critical information in support of situational awareness and decision making.
- Support public safety and security practitioners in their mission to protect Canadians.
- Anticipate, prepare for, and counter the emergence of future threats.

7.2.6. Canadian National Energy Board

NEB is an independent federal regulatory agency comprised of nine commissioners that addresses construction and operation of international and designated interprovincial transmission lines, imports/exports, and many other responsibilities related to natural gas and oil.[350] NEB enforces NERC reliability standards on the transmission lines it regulates.

7.2.7. Canadian Department of Justice

The Department of Justice supports the efforts of the Minister of Justice/Attorney General of Canada and the rest of the government in relation to national security. Its roles include:[351]

- Providing in-house legal services to other departments and agencies working in the field of national security, which includes giving consistent and effective strategic legal advice on national security law issues.
- Providing specialized constitutional, administrative access to information, privacy, human rights, and international legal advice on national security issues.
- Coordinating and conducting litigation involving the government, including with respect to national security issues.
- Providing policy advice and assisting in the development, drafting, and implementation of domestic legislative, regulatory, or other measures to protect national security and to combat terrorism.

7.3. State and Provincial Entities

7.3.1. State entities

A forthcoming jurisdictional study under preparation by DOE/OE identifies roles and responsibilities at the state level. Those that are most likely to have an impact on grid security are identified in the list below, along with others identified by state-level

reviewers of this report. All of these responsibilities are generalizations to account for variations by state as the states have a mix of Public Utilities Commissions (PUCs), Public Service Commissions, Corporation Commissions (in Arizona and Oklahoma), and other entities that regulate distribution services. Some states regulate municipally owned electric utilities and/or electric cooperatives in addition to investor-owned utilities (IOUs).

- Policy makers (Governor, Legislature)
  - The state governor and legislative bodies establish the overarching legal and regulatory framework for electricity sector operations in their states (authority derived from the U.S. Constitution, Federal Power Act, and on precedent set by *Munn v. Illinois* (1877)] allowing for states to regulate private entities that provide a service for the public good).
  - Establish and authorize PUC to regulate IOUs (via state statute).
  - Set state policies related to electricity or approve participation in regional activities.
  - Governor oversees emergency response efforts and controls the state's resources in the case of an emergency. In most states, the National Guard commander for the state will become the incident commander, and report to the governor.
  - Governors have the ability and authority to use National Guard units in their states, through a Title 32 designation, for state active duty status. This requires the concurrence of the President or Secretary of Defense, and can enable these units to have law enforcement types of functions as well, subject to control by the governor.
  - Jurisdictional authority only applies within state bounds, but state leaders often coordinate with regional and federal authorities (e.g., on interstate transmission siting or regarding environmental impact studies).
  - Some state commissions are elected (13 states) through direct elections every 4 years; however, in most states, commissioners are appointed by the governors and confirmed by the state Senate, and serve a term of 4 to 6 years.
  - Some state commissions are established in the constitutions of the states (e.g., California, Arizona); however, in most states, the statutory authorities for the commissions are established by the legislatures, and the commissions act as quasi-judicial (adjudication) and quasi-legislative (rule-making) authorities.
- The National Governors Association (NGA) is the bipartisan organization of the nation's governors, allowing governors to identify priority issues and deal collectively with matters of public policy and governance. Through NGA, governors share best practices, address national policy, and develop innovative solutions to key issues.[352] NGA's Homeland Security and Public Safety Division has been addressing cybersecurity, among other issues.
- Regulators (PUC) (responsibilities may be at the state, local, or tribal levels, in some cases)
  - Regulate a variety of critical infrastructures, which vary from state to state, but usually include retail electricity at the distribution level, intrastate natural gas, wireline communications networks, water and waste utilities (investor owned), and certain transportation functions. Thus, regulators are well positioned to

address the interdependencies of the critical infrastructures to cyber and physical events, such as the nexuses of communications-electricity, natural gas-electricity, and water-energy.

- Regulate all activities of IOUs providing services within the state and, in certain states, some actions by public power or cooperatives (established by state public utility acts or similar acts). The Federal Power Act effectively provides states with all regulatory authority that is not designated to FERC or other federal authorities.
- Regulate public power (municipally owned) entities in a small number of states. In the majority of states, a PUC only regulates public power entities operating outside the corporate limits of the municipality.
- In some states, approve or oversee low-voltage distribution lines siting and investments in distribution (e.g., meters, poles, wires).
- Possess general authority over the reliability of the transmission and distribution system in the state.
- Review and approve the capital investments and long-term planning of IOUs, including investments in generation and resource planning, where applicable.
- Review requests for proposals and the procurement decisions of utilities.
- Ensure that state resource mix policies and other state energy goals are carried out by regulated IOUs and enforce reserve margins.
- Have an obligation to ensure that power is both affordable (for low-income and senior citizens) and provided in a safe manner.
- Commissions may be the state sector-specific agency for ESF #12, requiring close coordination with all levels of government and industry.
- Responsible for cost recovery mechanisms for the investments in cyber and physical security that the utilities wish to make, applying traditional standards like prudency and usefulness. Other mechanisms that commissions can use to provide guidance on cost recovery include policy statements, use of future test years or significant use of pro forma adjustments, and performance-based measures.

- NARUC is the national association for the regulatory utility commissions and serves as a clearinghouse and educational body for the state commissions. NARUC has been active in cybersecurity, resilience, and black sky incidents over the past 5–10 years; has published papers on these subjects; and has engaged with other regulatory and policy bodies in discussions on security and resilience.
- Other key parties include:
  - Chief information officers, individually and through their organization—the National Association of State Chief Information Officers (NASCIO), have been increasingly active regarding cybersecurity, advanced cyber analytics, and digital privacy issues. In 2015, NASCIO published an overall Cybersecurity Awareness Resource Guide and, in 2016, they published a Cyber Disruption Response Planning Guide (both can be found at http://www.nascio.org/Publications), among many others.
  - State patrols and transportation departments participate in the activities of information and intelligence sharing, and state patrols may participate in law enforcement activities in the event of a specific incident related to critical

infrastructure. In many states, they also participate in the activities of the state fusion center. For physical security events, state transportation departments may play an important role in allowing the transportation of LPTs, restoration crews and equipment, and other first responders through state transportation corridors to arrive on the scene of the disaster or incident.

- Within the states, fusion centers and ISAOs offer important mechanisms for reaching stakeholders at a more local level. Some states, such as New Jersey, are developing integration cells to analyze the threats to, and the vulnerabilities of, infrastructure within a state, and develop timely and actionable threat alerts and warnings.

7.3.2. Provincial entities

The responsibility for ensuring bulk power system reliability in Canada rests primarily with the eight provincial governments; NEB also has reliability in its authorities.[353] Not all jurisdictions have the necessary legal structures to name an ERO, but NEB and most provinces recognize NERC as an electric reliability standards-setting organization and support NERC's standards-setting and oversight role as the North American ERO through legislation, regulation, orders in council, and memoranda of understanding (MOUs) or other agreements.[354] Each jurisdiction with NERC standards has a means to enforce compliance, such as ordering corrective actions; imposing reporting requirements; and, in some cases, levying financial penalties.[355]

Within each province, key parties in grid security typically include the following:

- Energy authority or ministry
- Resources agency
- Utilities commission or board
- Electric system operator or electricity coordinating council
- Primary utility serving the province, whether privately or provincially owned

There are significant variations by province, but this list indicates some of the key roles.[356]

Canada's Energy and Utility Regulators (CAMPUT, based on the original name of the group) is an organization of federal, provincial, and territorial boards and commissions responsible for the regulation of the electric, water, gas, and pipeline utilities in Canada. CAMPUT strives to improve public utility regulation in Canada, and improve the education and training of commissioners and staff of public utility tribunals; it is an affiliate of NARUC.[357]

7.4. Private Sector

The owners and operators of the equipment and infrastructure on the grid are primarily responsible for grid operation and security, whether they are IOUs, municipals, or cooperatives. They are responsible for implementing protection and mitigation measures and leading their response and recovery activities. To support them, a number of

structures have been put in place, including the standards established by NERC and the information sharing and coordination of the Electricity Subsector Coordinating Council, the similar Energy and Utilities Sector Network in Canada, and other coordinating bodies.

7.4.1. North American Electric Reliability Corporation

NERC is a nonprofit international regulatory authority whose mission is to ensure the reliability of the bulk power system in North America, particularly the continental United States, Canada, and the northern portion of Baja California, Mexico (as a part of the Western Electric Coordinating Council). NERC is recognized as the ERO for North America, subject to oversight by FERC in the United States and provincial and federal authorities in Canada. NERC develops and enforces, where so designated, reliability standards; assesses seasonal and long-term reliability; monitors the bulk power system; and offers training and certification of industry personnel.[358]

FERC can approve or remand for modification a standard proposed by NERC. It can also order additional standards in particular areas. Individual provincial jurisdictions in Canada have varying authorities regarding the acceptance, rejection, remanding, or tailoring of NERC standards.[359]

7.4.2. Information sharing and coordination

In December 2003, Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection, first established a national policy for federal departments and agencies to identify and prioritize critical infrastructure and to protect them from terrorist attacks. It also identified the roles of various governmental agencies in addressing the directive. In 2013, PPD-21, Critical Infrastructure Security and Resilience, replaced HSPD-7, keeping much of what was previously set out, but adding a greater emphasis on cybersecurity and expanding it to formally address all hazards. Both directives recognized DOE as the lead agency for the energy sector, with responsibilities to work with DHS, other federal agencies, owners and operators, and other parties.

As part of responding to first HSPD-7 and then PPD-21, the National Infrastructure Protection Plan (NIPP) was developed. Released as an interim version in 2005 and a full version in 2006, with an update in 2009 and a total revision in 2013, the NIPP set out a number of partnership structures for coordination and information sharing within and across sectors, including energy. Some of the formal coordination and information-sharing councils available to the electricity subsector include:

- Electricity Subsector Coordinating Council (ESCC): Represents the interests of the industry and is composed of electric utility industry executives. It is the principal mechanism for private sector owners and operators to work collaboratively with the government under a structured and protected framework that allows open dialogue. There is a counterpart subsector coordinating council for the Oil and Natural Gas Subsector. Numerous task forces and subcommittees have worked on supply chain concerns, interdependencies, and coordination with other sectors. The ESCC is also a critical coordination mechanism for information sharing during and after incidents.

To support the deployment of tools, improve the flow of threat information, prepare for incidents, and work closely with other infrastructure sectors, the ESCC has established four standing committees:

- "*Industry-Government Coordination:* Unify industry and government efforts to plan and prepare coordinated responses to incidents affecting grid security.
- *Leveraging Infrastructure / Research & Development:* Guide infrastructure investments and R&D to encourage the more efficient deployment of critical infrastructure protection tools and technologies.
- *Threat Information Sharing & Processes:* Improve and institutionalize the flow of, and access to, threat information among public- and private-sector stakeholders.
- *Cross-Sector Coordination:* Develop strong partnerships among electricity and other critical infrastructure sectors (communications, transportation, financial services, water, and downstream gas) to plan and respond to major incidents, better understand and protect our mutual dependencies, and share information effectively."[360]

- Energy Government Coordinating Council (EGCC): This government counterpart to the ESCC is jointly led by DOE and DHS, with membership from all levels of government and international partners.

These structures are mirrored for the other sectors called out in PPD-21, and collectively serve as a means of sharing information, best practices, research needs, and other critical infrastructure security and reliance information, such as information about interdependencies, across sectors.

Other information-sharing mechanisms include:

- NERC has established a Critical Infrastructure Protection Committee (CIPC) that addresses specific issues related to NERC's security initiatives and protection of the electric system. CIPC is composed of cyber, physical, and operational security experts from industry and also includes both DOE and DHS.
- Other industry trade associations important to coordination and collaboration include EEI, the National Rural Electric Cooperative Association, and the American Public Power Association in the United States.[361] In Canada, the primary association is the Canadian Electricity Association (CEA), which has an active program on cyber and physical security. It also coordinates with EEI on the activities of the ESCC, and coordinates directly with Canadian federal agencies. Trade associations can help build consensus and provide powerful communications channels.
- The Electricity Information Sharing and Analysis Center (E-ISAC) provides security services to its members—electricity service owners and operators in the United States, Canada, and portions of Mexico—and is operated by NERC. Some of its services include gathering and analyzing security information; providing indicators of grid compromise; physical security advice; and training on physical initiatives, technologies, and evolving trends.[362]
- The Cybersecurity Risk Information Sharing Program (CRISP) is a voluntary program to facilitate the exchange of detailed cybersecurity information among electric utilities, E-ISAC, DOE, and the Pacific Northwest National Laboratory to enable

electric power critical infrastructure operators to better protect their networks from sophisticated cyber threats.

- The North American Transmission Forum (NATF) includes investor-owned, state-authorized, municipal, cooperative, U.S. federal, and Canadian provincial utilities. NATF promotes the open and candid exchange of information among its members to improve the reliability of the transmission systems in the United States and Canada. Four guiding principles—community, candor, commitment, and confidentiality—give NATF the ability both identify and proactively address key reliability, security, and resiliency issues.[363]

In Canada, the National Strategy for Critical Infrastructure sets the direction for enhancing the resilience of critical infrastructure against current and emerging hazards.[364] It recognizes that timely information sharing across government and industry is needed to "promote effective risk management and to understand and address critical infrastructure interdependencies."

Sector networks connect federal departments and agencies with critical infrastructure partners from the provinces, territories, national associations, and industry to:

- Promote timely information sharing.
- Identify issues of national, regional, or sector concern.
- Provide sector-specific, subject matter expert guidance on current and future challenges.
- Develop tools and best practices to strengthen critical infrastructure resilience across the full spectrum of prevention, mitigation, preparedness, response, and recovery.

Electric utilities and CEA are members of the Energy and Utilities Sector Network, co-chaired and facilitated by NRCan.

A National Cross-Sector Forum, organized by PSC, promotes information sharing across the sector networks and addresses cross-jurisdiction and cross-sector interdependencies. Members comes from the 10 sector networks and include owners and operators; associations; and federal, provincial, and territorial governments.

In addition, Canadian companies often participate in the U.S. coordinating councils and other forums.

8. Financial and Insurance Incentives

Another key role in promoting the security and resilience of the grid is that of the financial and insurance markets. Electric grid infrastructure must continue to be developed, constructed, operated, and maintained to not only meet current and future demands, but also to overcome evolving threats and other challenges. This section provides a brief discussion of various financial mechanisms and incentives pertaining to electric grid security and resilience. Specifically, the following topics are examined:

- Insurance's role in grid security
- Federal government's roles in insurance and other incentives
- State governments' roles in insurance and cost recovery
- Cyber insurance
- Catastrophe bonds

Other financial incentives may come in the form of grants—these are not addressed here. Much of the experience to date comes from addressing natural disasters or terrorism.

8.1. Role of Insurance in Electric Grid Security

In the United States, insurance is one of the principal risk management instruments, not only for aiding in recovery after a disaster, but also for encouraging future investments that are more resilient to potential hazards. Many risks facing the U.S. electric infrastructure are covered by the insurance industry, which provides financial compensation mechanisms against selected risks. While this does not technically reduce actual disaster consequences or reduce hazard likelihood, owners and operators can choose to manage risks by accepting, mitigating, or transferring them through insurance.[365]

Accepting risk, often practiced through self-insurance, is optimal when the costs of mitigation and risk transfer are too high relative to the perceived probability and magnitude of loss. Large electric utility owners and operators often choose this option if purchasing third-party insurance is too costly, the perceived risk is small, or the risk is so new that it is not well understood.

Utility owners and operators can reduce losses through integrative risk management approaches. However, risk mitigation through prevention, the hardening of assets, and effective remediation may involve investments that are costly.

Risk transfer generally refers to third-party insurance. The sharing or spreading of risks over time and over a large group allows for the financial consequences of a disaster that occurs to be shared by a large group of people, rather than the burden falling only on the affected individuals or communities.

8.1.1. Insurance for electric grid security

Currently, insurance plays an important but limited role in the electricity sector. In general, insurance in the electricity sector is geared toward the standard operational

functions of business, consumer lawsuits (e.g., injuries from falling equipment or power lines), and property damage (e.g., house/roof damage from fallen power lines).

[366] Therefore, insurance in the electricity sector is designed to reduce liability and is not necessarily designed to promote protection or prevent catastrophic or terrorist-related damage to the electricity infrastructure.[367]

In addition to large, well-known insurers, most large utilities participate in a large mutual-risk pool called Associated Electric & Gas Insurance Services Limited (AEGIS). AEGIS is a mutual insurance company owned by its policyholders that is said to represent "virtually the entire energy infrastructure in North America, including gas and electric utilities, related energy companies, oil & gas exploration and production companies, water utilities, and transmission & distribution companies."[368] AEGIS provides liability and property coverage, as well as related risk management services.

In the electricity sector, insurance offerings for transmission and distribution (T&D) is limited because of jurisdictional issues related to T&D assets that are geographically dispersed. Repair or replacement is not only considered part of doing business for a utility, it is cheaper than purchasing an insurance policy.[369] Furthermore, typical T&D "equipment failures and damage and subsequent outages are subject to an outage and risk profile that is self-insured by electric utilities."[370] Although T&D lines are generally uninsured, transmission substations (e.g., power transformers) that are integral to the T&D systems are insured. Hartford Steam Boiler, a subsidiary of Munich Re, is one of the largest providers of equipment breakdown insurance, including for power transformers.[371]

8.2. Federal Government

The U.S. government often bears the key responsibility for risk mitigation in society beyond that which the private sector will cover, and governmental organizations at all levels—federal, state, local, tribal, and territorial—share the common goal of preventing or lessening the effects of disasters.

The federal government engages in a wide variety of insurance activities and has assumed insurance risks for at least two reasons: (1) the government may step in when insurance is not widely available because private insurers cannot collectively absorb or affordably price the insurance risk, or (2) the federal government has self-insured—that is, elected to pay for losses itself when it has determined that doing so is preferable to purchasing insurance in the private market.[372] The federal government operates at least 157 programs through 30 different organizations that provide insurance-like benefits to individuals and businesses, generally for natural disasters.[373]

The government plays a vital role in ensuring the viability of private insurance by creating appropriate legislative and regulatory frameworks. While the federal government retains the authority to regulate insurance, the primary responsibility for insurance regulation lies with the states, in accordance with the McCarran-Ferguson Act of 1945.[374, 375] According to this Act, state insurance commissioners are responsible for most aspects of insurance regulation.

8.2.1. Federal Terrorism Insurance Program

Following the September 11, 2001, attacks, President George W. Bush signed into law the Terrorism Risk Insurance Act (TRIA) in November 2002 to address the risk of terrorist attacks. Title 1 of TRIA created a temporary Federal Terrorism Insurance Program (FTIP) to help the insurance market recover from 9/11 and create a transitional period for private insurance markets to stabilize and develop solutions for covering losses due to terrorism.[376] As a result of the major losses resulting from 9/11, many reinsurers left the terrorism market, forcing primary insurers to do the same. Therefore, the U.S. government enacted TRIA, requiring insurers to offer terrorism coverage, with the government acting as a reinsurer.

Specifically, FTIP requires insurers to make available terrorism risk insurance for commercial property and casualty losses resulting from certified acts of terrorism, and provides for shared public and private compensation for such insured losses.[377] FTIP is activated when losses from certified acts of terrorism exceed $100 million in a fiscal year.[378] Although it was meant to be a temporary solution, TRIA has been reauthorized a number of times since 2002. Most recently, President Obama signed the Terrorism Risk Insurance Program Reauthorization Act of 2015 (H.R.26) on January 12, 2015, extending the program through December 31, 2020.[379]

8.2.2. FERC rate recovery

In the United States, both federal and state governments have the authority to oversee the electricity industry. At the federal level, FERC regulates rates for wholesale electricity sales and transmission of electricity in interstate commerce, including recovery of the costs of investments that utilities make to enhance security. However, FERC's ability to encourage security investment through rate recovery is limited to investor-owned utilities participating in wholesale transactions. Utilities operating in a competitive wholesale electric market are not required by FERC to make investments to enhance security.[380]

FERC has made a policy statement following 9/11 that it "approve[s] applications proposing the recovery of prudently incurred costs necessary to further safeguard the nation's energy systems and infrastructure."[381] FERC further stated in its fiscal year 2005 Congressional Performance Budget Request that it would give its highest priority to processing any filing made for the recovery of extraordinary expenditures to safeguard the reliability of energy transportation systems and energy supply infrastructure.[382] It is unclear, however, if any transmission owners have filed formal requests for security cost recovery.[383]

8.2.3. FERC enforcement of reliability standards

The FERC Office of Enforcement plays an important role in maintaining and enhancing the reliability of the U.S. electric grid.[384] Working closely with NERC, FERC focuses on "violation[s] resulting in actual harm, either through the loss of load or through some other means, as well as cases involving repeat violations of the reliability standards or a violation of a standard that carries a substantial actual risk to the system."[385]

Electric utilities who fail to comply with the NERC Reliability Standards are subject to penalties and sanctions, which can range from $1,000 to $1 million per day, per violation.[386] According to FERC's 2015 Report on Enforcement, in fiscal year 2015, FERC opened 19 new investigations and brought 22 investigations to closure.[387] The most notable settlements in fiscal year 2015 concerned the September 2011 blackout in the southwestern United States, which affected Arizona; Southern California; and Baja California, Mexico. The blackout had a substantial impact on the economy and citizens of affected areas of both countries, including power loss to millions of people, closure of schools and businesses, and disruption to flights and public transportation. Although a significant portion of the civil penalties was offset by the companies' agreement to invest in reliability measures designed to improve the reliability of the Western Interconnection, their fines in civil penalties reached a total of $23 million and disgorgement of nearly $1 million in unjust profits.[388]

8.3. State Government

While the bulk power system is regulated by NERC and FERC, the portions of the electric grid containing distribution systems are subject to regulation by state PUCs. Specifically, the regulatory processes for recovering investment costs in utility infrastructures in many states are handled through rate-of-return regulation and other cost-recovery mechanisms.[389] In states with a regulated electricity market, PUCs approve investment costs related to infrastructure security and determine how such costs can be recovered.[390] In some states, however, cost recovery for investments made for security enhancements could be difficult as some states have imposed rate caps.[391]

While new legislation or regulatory proceedings have been developed to deal with cost recovery of security-specific investments, more typically existing regulatory cost-recovery mechanisms are used. Many of the cost-recovery protocols involve some form of a rate case proceeding, which requires that a recoverable cost be just and reasonable.

In addition to being a regulator, states also offer a wide variety of public insurance programs. Although state-regulated disaster insurance programs have continued to grow, they are also facing a number of challenges. Critics of state-regulated disaster insurance programs have argued that insurance prices and terms of coverage are highly regulated and that the insurance industry is generally not allowed to respond freely to changing risks or market conditions. The result, it is argued, is that some states are creating a significant financial exposure that sometimes may not be covered by the revenues that they earn through low-priced insurance policies. According to a recent analysis by the Insurance Information Institute in 2011, more than 35 programs nationwide had grown to provide a record high of 3.3 million policies, many of which are in high-risk regions.[392]

8.4. Cyber Insurance

Cyber insurance refers to a relatively new type of insurance product covering a broad range of issues related to risk in cyberspace, with typical issues including liability, property loss, theft, data damage, and loss of income from network outages and

computer failures or website defacement.[393] In general, most businesses purchase a package of insurance policies called the business owner's policy, which typically includes property insurance, business interruption insurance, and liability protection.[394] However, none of these policies covers data breaches or anything data related, due to what is known as the "intangible property exclusion."[395] Yet the average cost of a data breach is rising for companies around the world, estimated at $3.8 million in 2015, up from $3.5 million a year earlier.[396] Despite this, surveys show that a majority of businesses still do not have a cybersecurity policy, which suggests that cybersecurity risk is underinsured.[397]

In general, insurance policies contain two types of coverage—first-party losses, which refer to direct losses sustained by the insured through cyber-related activities, and third-party losses, which concern a company's liability regarding losses sustained by third parties caused by the insured's cybersecurity incident.[398] While these characteristics describe the typical components of cyber insurance, cybersecurity risk is such a broad area that any insurance policy has to be tailored to the specific risks facing each organization. Consequently, insurance products first introduced to market have been mostly customized.[399]

Several unique attributes of cybersecurity risk present challenges in the development of cyber insurance, including the following:[400, 401]

- Cyber risk is difficult to measure, model, and price due to a lack of actuarial data.
- Cyber attack is an intangible threat, and it is difficult to measure the likelihood and/or consequences of a cyber-related service outage involving a cloud or third-party service provider.
- It is difficult to take into account and understand the various interconnected activities as digital networks and shared technologies form connections that can be exploited to generate widespread impacts.
- Cyber risk is a dynamic, evolving threat, which is not constrained by the "conventional boundaries of geography, jurisdiction or physical laws."[402]

Despite these challenges, cyber insurance is a rapidly growing market. The current global cyber insurance market is estimated to be worth around $2 billion in premiums, with U.S. businesses accounting for approximately 90 percent.[403] The cyber insurance market is expected to triple by 2020, growing to $7.5 billion;[404] another source estimated that the market will reach $20 billion by 2025.[405]

A recent study by Lloyd's suggests that insurers could be required to meet claims across many different classes of coverage (including power generation companies, companies losing power, companies affected by supply chain interruptions, homeowners, and others), emphasizing the importance of exposure management across the full set of insured entities. Additionally, there is a challenge for insurers in assessing risk exposure, both at the individual entity level and across all insured entities. Another challenge for assessing risks is the need for insight into the evolution of the tactics and motives of attackers. All of these impact the development of new cyber insurance products, while at the same time, insurance is needed to enhance cybersecurity and resilience.[406]

8.5. Catastrophe Bonds

Catastrophe bonds (commonly called "cat bonds") are financial instruments designed to help manage the financial risks associated with potentially devastating natural disasters, such as hurricanes, earthquakes, floods, and typhoons.[407] Similar to companies or organizations issuing bonds to raise capital, cat bonds are used by insurers and reinsurers to transfer major risks to capital market investors.[408] In short, cat bonds can allow governments and reinsurers to transfer the risk of large catastrophic losses from disasters to capital markets. As of the first quarter of 2015, the cat bond market was estimated to be worth about $25 billion, having grown 25 percent per year over the last decade.[409]

Economic losses from natural disasters have been on the rise in recent years, yet the vast majority of these losses have been uninsured. On average, only about 30 percent of catastrophic losses have been covered by insurance between 2004 and 2014, which means that governments and individuals have absorbed a growing share of the costs for disaster recovery of 70 percent of the total catastrophic losses (approximately $1.3 trillion) during that period.[410] Financial entities have noted a significant growth potential and predicted that the cat bond market would reach "$50 billion by 2018 as part of the larger insurance-linked securities (ILS) market that will climb to $150 billion."[411] As the cat bond market continues to grow, an opportunity may exist for insurers and governments to catalyze investments in resilience-enhancing projects by connecting cat bonds to investment projects that are designed to reduce risk.

The role of public sector entities in the cat bond market has been growing, and cat bonds are now regularly used by government-sponsored insurance programs, including the California Earthquake Authority, Florida Citizens Property Insurance, Louisiana Citizens Insurance, Texas Windstorm Insurance Association, World Bank, New York Metropolitan Transit Authority (MTA), and Amtrak.[412]

Particularly, after Superstorm Sandy, New York MTA purchased a cat bond with a specific trigger level that if a storm surge reaches 8 feet at Battery Park in Manhattan, the bond pays out immediately. Such an insurance policy encourages owners and operators to focus on assessing and mitigating real risk, as opposed to political or other kinds of risk; induces the implementation of mitigation measures in order to receive a reasonable price; and expedites recovery by quickly making resources available following a disaster.[413]

Similarly, the creation of cat bonds may be considered for cyber risks, which are thought to be too big for the insurance industry. While cat bonds are one possible avenue of exploration, it is unclear how cyber risks could be securitized to be transferred to capital markets. Because cyber risk exposures have "so many moving parts and have the potential to be volatile," modeling probabilities and expected loss can be challenging.[414] Thus, some have suggested government support may be needed to provide the financial backstop that companies need against cyber risks.[415]

TRIA is such an example of government-backed insurance because terrorism is considered to be an uninsurable risk. Sources have noted that cat bonds would not be created for risks that are not underwritten by the traditional reinsurance market.

[416] Thus, without the federal government's commitment to support terrorism risk through TRIA, the reinsurance community would not have the confidence to offer terrorism reinsurance. This explains why "there have been no securitizations of property-catastrophe bonds solely for terrorism risk in the market" to date.[417] This is an area that is expected to evolve as more experience is gained with cat bonds.

9. Issues Specific to North American Grid Security

9.1. Geographic Complexity

The complexity of securing the North American bulk power grid starts with the size of the grid. It covers all of the continental United States and Canada, as well as the northern portion of Baja California, Mexico. Cascading failures are somewhat limited by the details of the grid and its connections. Specifically, the North American grid includes three independent power grids operating in the continental states and adjacent parts of Canada, and some portions of Mexico: (1) the Eastern Interconnection (generally, states and provinces east of the Rocky Mountains), (2) the Western Interconnection (from the west coast to, and including, the Rocky Mountain states and provinces), and (3) the Texas Interconnected System. These systems are generally independent from one another, with limited links between them. Significant portions of Canada are interconnected with the United States through the Eastern and Western Interconnections, while parts of Mexico have limited connections to the Texas Interconnected System and the Western Interconnection. Alaska, Hawaii, and the northern part of Canada have one or more independent systems.[418]

There are efficiencies in such a large grid. Because there are shared threats and vulnerabilities, the impacts of any security event are likely to cross borders. Even if the direct consequences of an event do not cross borders, there will still be shared impacts, given the many ways in which the three countries interact for trade, transportation, and other activities. In some events, outages and their impacts cascade across the borders, as in the 2003 blackout.[419] The geographic and climatic features of the three countries can also create interdependencies, such as droughts or low-water situations in Canada affecting grid reliability in the western states of the United States. Weather can also affect the import/export balance among the countries.

9.2. Asset Ownership and Operation

In addition to the geographic complexity, the fact that the majority of the utilities are investor owned, as opposed to state or national ownership in many other countries, changes the dynamics of achieving interoperability and interchangeability, as well as instituting voluntary improvements to enhance security and resilience. Priority setting is done by company, not across the entire grid. Further complexity is added by having cooperatives and municipally owned utilities in the overall mix, which have their own mechanisms for setting priorities and making changes. This makes for a very large number of stakeholders who need to be coordinated with, involved in two-way communications, and informed of threat assessments and other analyses and warnings. As discussed in Section 7, numerous coordination structures and defined roles and responsibilities help address this, but this is a critical ongoing element of ensuring the security and resilience of the grid.

9.3. Regulatory Authorities

NERC covers the full territory of the grid, providing centralized reliability planning and a shared regulatory regime, and setting common standards and enforcing them in the United States. For the United States, FERC has authority over the electric reliability of the U.S. portion of the bulk electric supply. In Canada, regulatory oversight of electric reliability rests primarily within the jurisdiction of the provinces, while federal jurisdiction covers permitting of international exports and the construction and operation of international power lines and designated interprovincial power lines. The provinces determine the assignment of authority to enforce the NERC standards.[420]

9.4. Federal Leadership

DOE and NRCan have the primary roles in grid security under each country's emergency management and preparedness frameworks; however, the roles and responsibilities of the government and the private sector have subtle differences between the countries. DOE and NRCan collaborate under the auspices of the Canada-U.S. Clean Energy Dialogue and the 2014 MOU on Enhanced Energy Cooperation (as well as subsequent MOUs with both the United States and Mexico). The latter includes a focus on enhancing the reliability and security of the North American energy infrastructure.[421]

NRCan-DOE MOU on Enhanced Energy Collaboration

"On September 18, 2014, Greg Rickford, Canada's Minister of Natural Resources and Dr. Ernest Moniz, United States Secretary of Energy, signed an MOU launching an agreement on enhanced energy collaboration between Natural Resources Canada (NRCan) and the U.S. DOE. The signing continues a long and productive history of Canada-U.S. collaboration on a wide range of energy issues and shared interests in greater energy security, environmental responsibility and sustainability. Under the MOU, Canada and the U.S. plan to cooperate on initiatives, including sharing of knowledge, technical information and research plans to improve environmental practices in conventional and unconventional oil and gas development; enhancing the reliability and security of North American energy infrastructure; supporting the advancement of an efficient and clean electric grid; enhancing coordination on energy efficiency standards; facilitating increased use of natural gas in the transportation sector; collaborating to reduce the cost of carbon capture and storage (CCS); and engaging in regional and multilateral dialogues on energy and environmental issues to advance shared priorities."

Source: Natural Resources Canada, "After the Blackout: Implementation of Mandatory Electric Reliability Standards in Canada," paper presented at the Energy and Mines Ministers' Conference, Halifax, Nova Scotia, 2015, p. 14, https://www.nrcan.gc.ca/sites/www.nrcan.gc.ca/files/www/pdf/publications/emmc/15-0137%20EMMC-After%20the%20Blackout-e.pdf.

The countries generally work well together due to a long history of collaboration, both under routine conditions and in emergencies when there is a common goal of protecting people and property, and restoring service as quickly as possible.[422] Mutual assistance programs span the borders, but can face issues with regard to language, import/export requirements, work permits and border paperwork, and so forth.[423] To the extent feasible, most of these are worked out in advance; however, problems can still occur.

9.5. Resource Trends

There are different resource issues and trends facing the three countries, individually or collectively:

- Construction of new transmission lines to import/export electricity between Canada and the United States has numerous challenges.
- Natural gas is increasing in its use as a generation source, as discussed earlier. The United States exports gas to Mexico, which, in turn, exports power to southern California. There are also numerous Canadian gas pipelines exporting gas to the United States. The interdependence between gas and electric as the two become more integrated adds to the vulnerabilities that can affect the electric grid (and natural gas operations and transportation).
- Renewable sources are also increasing in importance across the grid as the use of non-renewable resources changes.
- Both the United States and Canada have a mixture of traditional, vertically integrated utilities and wholesale electric power markets.
- ICT is becoming increasingly important in both the United States and Canada.

These factors change the vulnerabilities of the grid and the consequences of any security event that might occur. Protection and mitigation efforts, as well as response and recovery plans, must be kept current with the changing nature of the grid overall and within each country.

10. Lessons Learned From Other Nations and Events

Although the North American grid has a number of unique elements, there is still much to be learned from both major incidents that have occurred worldwide and the best practices of other countries in enhancing the security of their grids. There are also a number of improvements made in the United States in response to catastrophic storms that provide additional examples of ways to improve the resilience of the grid from a security perspective.

10.1. Cascading Outages

A lightning strike in Brazil in March 1999 knocked out power to 97 million people, including people in São Paulo and Rio de Janeiro, when it struck a substation and caused a chain reaction. The outage was the worst in 15 years for Brazil.[424] India and Indonesia have had events between 2001 and 2012 that have affected 120–700 million people per event. Causes of the events have been cited as overdrawing of electricity by certain states and weak inter-regional power transmission corridors, failure of a substation combined with poor and inadequate transmission equipment, and failure in a transmission line; however, restoration generally occurred within 24 hours.[425]

The event in India in 2012 has been cited as the largest case of unsuccessful mitigation of cascading outages. While the cause of an initial outage was still under investigation, "a severely weakened system coupled with large unscheduled interchanges led to highly loaded tie lines. Load encroachment (apparent impedance entering the protective zone) tripped these tie-lines after inadequate operator relief actions. The resulting power swings split-up the system where lines continued to trip from under-frequency/over-voltage actions which eventually caused total collapse of all three grids."[426]

A review of North American outages in 2003 stated that the primary root causes could be attributed to (1) lack of investments in the grid, leading to bottlenecks in transmission; (2) lack of communication among operators; (3) a need for additional regulatory guidance for the operation of transmission systems and power plants in the case of cascading events; and (4) weak points in system protection, energy, and demand-side management.[427] A review of a major outage in Italy later that year found that "power systems have not been designed for 'wide-area' energy trading with load patterns varying daily." The event resulted in an action plan that included studying the settings of protection devices, reassessing the consequences of various systems, better coordination of emergency procedures, additional training on emergency procedures, further studies on integrating stability issues in security and reliability policy, reassessing acceptable overload margins, and studying real-time monitoring of transmission line capabilities. Overall, the study determined that hybrid AC/DC systems would provide better controllability of the power flows and assist in the prevention of cascading disturbances.[428]

A recent Institute of Electrical and Electronics Engineers (IEEE) paper focuses on mitigating and preventing cascading outages. It recognizes that visualization of cascading outages and potential control actions improves both the situational awareness of operators and their preparedness to address events. The research finds that a lack of coordination in key areas is a common problem, particularly across transmission system operators (TSOs) in an interconnected region. The paper suggests the importance of increased coordination among TSOs in terms of protection settings, real-time exchanges, system studies and planning and role in an emergency state, and system conditions, as well as such coordination within regions. The authors also note the need for operator training on emergency states so that they can grasp the situation and take appropriate actions quickly. The authors indicate that a lack of urgency was in play with regard to the severe consequences of the 2003 blackout in Italy. Italy and India were also cited as having a common problem with regard to exchanges across interconnections, particularly with larger than agreed upon imports overtaxing the systems. Lastly, they recognize the importance of synchrophasors and ICT to minimize the impact of cascading failures, but recognize the challenges of converting large amounts of data into actionable information.[429]

Another paper, developing an approach to modeling any type of interdependent networks, used examples from electric grids around the world. In one case, they pointed out how the Italian blackout in 2003 cascaded when the shutdown of power stations disabled nodes in the Internet communication network, and then this caused further failures of power stations, all in a chain of power station(s) and communications node(s).[430]

10.2. Other International Events

Two other South American blackouts (Brazil in 2001 and Chile in 1999) also provide insight into needed mitigations.

A major energy shortage and blackouts occurred in Brazil in 2001, when droughts over the preceding years dropped the amount of hydroelectric generation—Brazil's source for 90 to 95 percent of its electricity generation. Numerous authors were cited as attributing the crisis to "the lack of investment in new generation capacity, unfavourable grid development, and incomplete legislation, as well as a lack of flexibility in planning and delay in the adjustment of the rules before and during the crisis. There was no appropriate incentive scheme in place for the new capacity building which later resulted in the shortage of supply." One of the referenced reports pointed to ineffective government, insufficient intra-government communications, a lack of clear responsibility for overseeing energy policy, and incomplete and inadequate legislation, among other causes.[431]

In 1999, Chile also had an energy shortage and blackouts due to reduced hydroelectric power, resulting from reduced water levels: The very low levels were due, in part, to both a government and power and water prices that were not properly responsive to the environmental conditions and supply. Less reliance on hydroelectric generation would also minimize such impacts.[432]

10.3. International Cybersecurity Events

The December 2015 unscheduled outage in Ukraine has been discussed in both Sections 2 and 4 of this report. The event resulted from a cybersecurity event, consisting of remote cyber intrusions at three regional electric power distribution companies. The three intrusions occurred within 30 minutes of each other and impacted multiple central and regional facilities. The key action was malicious remote operation of the breakers, either through operating system-level access to remote administration tools or ICS software via VPN connections. It is believed that legitimate credentials were obtained prior to the events. Expected restoration efforts were deliberately impaired by erasing key files, corrupting firmware, and scheduling uninterruptable power supply (UPS) disconnects.[433]

Mitigating such cybersecurity events requires the implementation of information resources management best practices, including procurement and licensing of trusted hardware and software; knowledge of software, hardware, and users on the system; implementation of patches as available; and strategic refreshes of technology. Numerous other measures and best practices ensure that the opportunity and ability to upload and execute malware is limited, ICS networks are protected, and remote access is both limited and has multi-factor authentication.[434]

This was the first publicly acknowledged cybersecurity event to result in a power outage. As power outages go, this was relatively small (225,000 customers) and short (several hours). However, it is indicative of what trained attackers can do remotely to integrated cyber-physical systems. The attacker obtained credentials and remote access, operated control systems, knew how to disable critical equipment, and then knew how to constrain and delay restoration operations. The event pointed out the types of information that are readily accessible. The E-ISAC report on the event provides guidance that goes beyond the Ukraine event, considering what it will take to defend against the next event, which will learn from the event in the Ukraine and try to defeat the protective measures taken by utilities. These suggested practices address spear phishing, credential theft, data exfiltration, VPN access, workstation remote access, control and operations, tools and technology, and response and restoration. More than 20 recommendations are made on architecture, passive defense, and active defense.[435]

10.4. International Experience With Physical Grid Events and Accidents

To date, physical security events targeting elements of the North American electric transmission and distribution system consist of small-scale vandalism executed by a few individuals or small groups, generally with limited technical sophistication. Internationally, events targeting the transmission and distribution system or other parts of the electric system have been considerable. Successful events at generation plants have occurred in Baghdad. In Colombia, efforts to impact generation were prevented due to high levels of security that can be concentrated on individual targets. Because security for extended and dispersed/isolated systems is more difficult, most of the security events have been focused on transmission and distribution systems.[436]

While not a malicious event, this next accidental event also illustrates the consequences that could occur from a deliberate event targeting certain systems. In November 2006, as previously planned, a transmission line was taken out of service to let a boat pass under it. However, a serious system disturbance originating from the North German transmission grid as the line was taken out of service impacted the interconnected power systems of the Union for the Coordination of the Transmission of Electricity (UCTE) synchronous area, involving large parts of the European power systems. After the tripping of many high-voltage lines, the UCTE grid was divided into three geographic areas and significant power imbalances and frequency deviations resulted in each area.[437] Before and during the event, safety limits and protection schemes were not uniform or communicated to other TSOs, some TSOs were not aware of the location of the disconnected point or the reason for it, and a lack of real-time communications among TSOs was also evident.[438] A post-event evaluation determined the need for an improved legal and regulatory framework to minimize the consequences of future events, and greater coordination and cooperation among TSOs. This latter area should include the following:[439]

- Coordinated real-time security assessment and control
- Exchange of real-time data among neighboring TSOs, based on the harmonization of data standards
- Joint operator training programs and decision support systems

10.5. Lessons Learned From Recent U.S. Storm Experience

In the aftermath of Superstorm Sandy, Hurricane Irene, and Tropical Storm Lee, Governor Andrew Cuomo convened the NYS 2100 Commission. The Commission focused on natural disasters; however, many of the nine key recommendations have significant bearings on improving the security of the grid as well:[440]

1. Protect, upgrade, and strengthen existing systems.
2. Rebuild smarter: Ensure replacement with better options and alternatives.
3. Encourage the use of green and natural infrastructure.
4. Create shared equipment and resource reserves.
5. Promote integrated planning and develop criteria for integrated decision making for capital investments.
6. Enhance institutional coordination.
7. Improve data, mapping, visualization, and communication systems.
8. Create new incentive programs to encourage resilient behaviors and reduce vulnerabilities.
9. Expand education, job training, and workforce development opportunities.

The Commission's recommendations for the energy sector all impact security, with some key points noted below the recommendations:[441]

1. Strengthen critical energy infrastructure.

   Create a long-term capital stock of critical equipment to streamline recovery processes.

2. Accelerate modernization of the electrical system and improve flexibility.

   Re-design the electric grid to be more flexible, dynamic, and responsive.

   Increase distributed generation statewide.

3. Design rate structures and create incentives to encourage distributed generation and smart grid investments.

   Implement new technologies and system improvements to provide effective backup power, flexibility, distributed generation, and solutions for "islanding" vulnerable parts of the system.

4. Diversify fuel supply, reduce demand for energy, and create redundancies.

5. Develop long-term career training and a skilled energy workforce.

   The recommendation discusses coordinating workforce development across the energy sector, which will help prepare for, and respond to, emergencies, particularly involving advanced technologies.

The New York Power Authority (NYPA) then released its Strategic Plan, noting that infrastructure changes will be driven by the following:

- Development of new technologies such as solar power, electric vehicles, and the smart grid
- Awareness of environmental issues
- Changes in the structure of energy markets, economic growth, and new demands for energy

This helps incorporate many of the recommendations of the NYS 2100 Commission into the path forward for the state.[442]

11. Conclusions and Next Steps

Concerns about the security of the electric grid in the face of adversarial threats are widely recognized and shared. The fundamental issue at stake is to determine next steps for improving grid security and how to prioritize these steps among all of the other issues that face the industry.

- **Additional threat and risk information.** Utility owners and operators, whether investor-owned, municipal, or cooperative, generally are responsible for making system improvements. However, without timely and specific information on the ways in which equipment could be damaged or disrupted by adversarial threats, it is difficult for them to properly prioritize changes, upgrades, and mitigation efforts that could improve physical security. Utility executives are now understanding the business impact of cybersecurity, making it easier to justify improvements, at least in some cases. Actionable threat and risk assessments are needed to optimize owner/operator investments in both new technology and the replacement of aging infrastructure to improve security. These investments also need to be appropriately valued by state public service commissioners when they evaluate rate cases.
- **Integrating cyber-physical expertise.** The integration of cyber and physical systems is making major improvements in the ability to monitor and operate the grid and offering improved protection, but at the same time it is also introducing new vulnerabilities. To reduce existing vulnerabilities and minimize the introduction of new ones, we must integrate cyber and physical expertise into all stages of the research-develop-build-operate continuum. More integration is needed not just when new technology is introduced, but also when existing systems are upgraded or repaired because such changes can introduce unrecognized vulnerabilities if both overall systems and components are not evaluated before changes are made. Increased communications between technology developers, suppliers, integrators, and buyers on how the systems will be used, could help improve their understanding of security implications and, therefore, result in better solutions.
- **Understanding interdependencies.** Communications and coordination are important capabilities for identifying and understanding interdependencies and cross-sector work at the local, regional, and national levels. Convening regional webinars, taking advantage of existing industry and state government meetings, working with fusion centers, and conducting tabletop exercises (with coordinated follow up) are all ways to increase the identification and understanding of interdependencies, particularly about new infrastructure that may depend on and impact the grid and vice versa.
- **Research and development.** Significant research is underway on the design and development of new and improved grid technologies, much of it driven by investments to increase reliability, improve operational efficiency, and accommodate changing generation sources. Two areas warrant additional attention—both of which were noted in the Energy Sector-Specific Plan:[443]
  - A comprehensive framework for interdependency modeling and simulation to help (1) integrate the multiple and disparate models, tools, and simulations that already exist for different infrastructure; and (2) facilitate cross-sector analysis to address the threat assessment, protection, mitigation, response, and recovery issues associated with interdependencies.

- Additional tests and studies on the impact of GMD, EMP, and other physical threats on critical grid components, including LPTs and bushings, or greater sharing of the results of previous tests and studies with industry if they are sufficient.

  In addition, DOE is leading numerous research and development projects for both physical and cybersecurity, as shown in Table A-2. These projects span improvements in design, system architecture, communications, risk management tools, and training and exercises.

  Long-term research and development is needed to make grid technologies more resilient through more modular designs that support quick(er) replacement, more flexible and adaptable designs that speed recovery, self-healing systems to minimize outages and damage, and so forth. There is also a need for research and development to enhance response and recovery to adversarial incidents (as well as other types of incidents).

  Significant cybersecurity work is also underway through DOE's CEDS program designed to assist the energy sector asset owners (electric, oil, and gas) by developing cybersecurity solutions for energy delivery systems through integrated planning and a focused research and development effort. CEDS co-funds projects with industry partners to make advances in cybersecurity capabilities for energy delivery systems.

  Overall, it will take significant additional investment to outpace threats; this cannot be done by government alone, so government should explore policies to reduce barriers to industry investment in grid security.

- **Reducing institutional barriers.** Numerous institutional barriers are still impacting vulnerabilities, response and recovery options, and outage durations. The implications of the following on security and resilience for adversarial incidents need to be further examined so that barriers can be reduced when and where necessary: restrictions on switching fuels for electricity generation, changes in communications between electric and gas utilities due to deregulation, and limited pipeline networks in certain regions. Building trusted relationships on the state and federal levels is also key.
- **Prioritizing recommendations.** DOE, NRCan, and the electricity industry as a whole are inundated with recommendations for research, studies, and actions on a broad range of issues, including EMP, climate change, severe storms, LPTs, cybersecurity, DER, renewables, the smart grid, physical attacks, earthquakes, insider threats, and others. Many of these issues also impact the security of the grid, either directly or through the changes that would occur to make the grid more reliable. Rationalizing and prioritizing all of the different recommendations or groups of recommendations, even at a coarse level, could allow for the optimization of limited resources. There will never be perfect information and it is not possible to protect against every threat and hazard, but a measured approach based on risks and consequences would add clarity to the current confusion, where every issue is the most important issue. More focus on the key recommendations can hopefully also help guide further regulations to ensure that they are focused on areas with agreed-upon gaps as current regulations are more fully implemented.

- **Working on cost recovery and insurance mechanisms.** Cost recovery for security and resilience improvements is very much an area of active discussion across government and industry, and it needs to be part of an all-hazards context, just like the prioritization of recommendations. Security investments are critical to a secure and resilient grid, but they cannot overwhelm local utility rates. Close working relationships between federal and state regulators and federal standard-setting bodies will help achieve greater consistency in cost oversight.

  As discussed in Section 8, the available insurance options are limited and still evolving. The recent report by Lloyd's on the implications of a cybersecurity event in the United States provides insight into the changes needed in insurance for cybersecurity events, but many of the same issues pertain to insurance for widespread physical security events, such as EMP. Interestingly, the report points out the need for innovative collaborations drawing on multidisciplinary expertise, as mentioned earlier in this section, to develop new insurance products. Better data and modeling are also needed, including finding a means to share anonymized data on the frequency and severity of security events.[444]

Acronyms

Acronym	Description
AC/DC	Alternating current/direct current
AEGIS	Associated Electric & Gas Insurance Services Limited
AMI	Advanced metering infrastructure
APPA	American Public Power Association
BES	Bulk electric system
C2M2	Cybersecurity Capability Maturity Model
CAMPUT	Canada's Energy and Utility Regulators
CEA	Canadian Electricity Association
CEO	Chief executive officer
CFR	Code of Federal Regulations
CIP	Critical infrastructure protection
CIPC	Critical Infrastructure Protection Committee
CISA	Cybersecurity Information Sharing Act
CISPA	Cyber Intelligence Sharing and Protection Act
CRISP	Cybersecurity Risk Information Sharing Program
CRS	Congressional Research Service
CSIS	Canadian Security Intelligence Service
DBT	Design basis threat
DER	Distributed energy resources
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
DOJ	U.S. Department of Justice
DOS	U.S. Department of State
DRDC	Defence Research and Development Canada
ECPA	Electronic Communications Privacy Act
EDS	Energy delivery systems
EEI	Edison Electric Institute
EGCC	Energy Government Coordinating Council
E-ISAC	Electricity Information Sharing and Analysis Center

Acronym	Description
EMP	Electromagnetic pulse
EO	Executive Order
EPRI	Electric Power Research Institute
ERO	Electric Reliability Organization
ESCC	Electricity Subsector Coordinating Council
ESF	Emergency Support Function
FAST Act	Fixing America's Surface Transportation Act
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FERP	Federal Emergency Response Plan (Canada)
FIOP	Federal Interagency Operational Plan
FTC	Federal Trade Commission
FTIP	Federal Terrorism Insurance Program
GMD	Geomagnetic disturbance
HSPD	Homeland Security Presidential Directive
HVE	Home-grown violent extremist
ICE	Interruption cost estimate
ICS	Industrial control systems
ICS-CERT	DHS Industrial Control Systems Cyber Emergency Response Team
ICT	Information and communications technology
IED	Improvised explosive device
IEEE	Institute of Electrical and Electronics Engineers
INL	Idaho National Laboratory
IoT	Internet of Things
IOU	Investor- owned utility
ISAO	Information-sharing and analysis organizations
ISO	Independent system operator
IT	Information technology
kV	Kilovolt
LPT	Large power transformers

Acronym	Description
MDMS	Meter Data Management System
MOU	Memorandum of understanding
MTA	New York Metropolitan Transit Authority
NARUC	National Association of Regulatory Utility Commissioners
NAS	National Academy of Science
NASPI	North American SynchroPhasor Initiative
NATF	North American Transmission Forum
NCCIC	National Cybersecurity and Communications Integration Center
NEB	National Energy Board (Canada)
NERC	North American Electric Reliability Corporation
NGA	National Governors Association
NIAC	National Infrastructure Advisory Council
NICC	National Infrastructure Coordinating Center
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NOC	National Operations Center
NRCan	Natural Resources Canada
NRE	National response events
NRECA	National Rural Electric Cooperative Association
NREL	National Renewable Energy Laboratory
NYPA	New York Power Authority
NYS	New York State
OCIA	DHS Office of Cyber and Infrastructure Analysis (at DHS)
OE	DOE Office of Electricity Delivery and Energy Reliability
OEIS	FERC Office of Energy Infrastructure Security
OER	FERC Office of Electric Reliability
PG&E	Pacific Gas & Electric
PII	Personally identifiable information
PPD	Presidential Policy Directive
PSC	Public Safety Canada
PUC	Public Utilities Commission

Acronym	Description
RCMP	Royal Canadian Mounted Police
RMAG	Regional Mutual Assistance Groups
RTO	Regional transmission organizations
S&T	DHS Science and Technology Directorate
SAE	Society of Automotive Engineers
SCA	Stored Communications Act
SCADA	Supervisory control and data acquisition
SGIG	Smart Grid Investment Grant
SNRA	Strategic National Risk Assessment
SSA	Sector-Specific Agency
STEP	Spare Transformer Equipment Program
T&D	Transmission and distribution
TRIA	Terrorism Risk Insurance Act
TSO	Transmission system operator
UCTE	Union for the Coordination of the Transmission of Electricity
UPS	Uninterruptible power supply
U.S.	United States
USB	Universal serial bus
USC	United States Code
US-CERT	U.S. Computer Emergency Readiness Team
VCC	Voluntary code of conduct
VoIP	Voice over Internet Protocol
VPN	Virtual private network
WSJ	The Wall Street Journal

Appendix A: Government and Industry Actions

The importance of grid security is well recognized at all levels of government and across industry, as evidenced by the broad range of actions taken to date or planned for the near future by industry, government, academia, trade associations, and others. While it is impossible to comprehensively list and describe all relevant activities, this appendix lists a number of the key actions; additional details for many of them are provided throughout the rest of this report.

Many of the listed actions are active collaborations with partners across government and industry. In these cases, they are listed by the sponsoring body, but that does not diminish the importance of the ongoing collaboration.

Table A-1: Listing of Major Efforts

Type of Action	Specific Action or Program
Executive Branch	
Executive Orders and Directives	▪ EO 12656: Assignment of Emergency Preparedness Responsibilities ▪ EO 13603: National Defense Resources Preparedness ▪ EO 13636: Improving Critical Infrastructure Cybersecurity ▪ EO 13650: Improving Chemical Facility Safety and Security ▪ EO 13691: Promoting Private Sector Cybersecurity Information Sharing ▪ HSPD-5: Management of Domestic Incidents ▪ PPD-8: National Preparedness ▪ PPD-17: Countering Improvised Explosive Devices ▪ PPD-21: Critical Infrastructure Security and Resilience ▪ Canada's National Strategy for Critical Infrastructure ▪ Canada's Cyber Security Strategy ▪ Defence and Security S&T Strategy (Canada)
Standards and Guidance	NERC CIP Standards: *Subject to Enforcement* ▪ CIP-002-5.1 Cyber Security – BES Cyber System Categorization ▪ CIP-003-6 Cyber Security – Security Management Controls ▪ CIP-004-6 Cyber Security – Personnel & Training ▪ CIP-005-5 Cyber Security – Electronic Security Perimeter(s) ▪ CIP-006-6 Cyber Security – Physical Security of BES Cyber Systems ▪ CIP-007-6 Cyber Security – System Security Management ▪ CIP-008-5 Cyber Security – Incident Reporting and Response Planning ▪ CIP-009-6 Cyber Security – Recovery Plans for BES Cyber Systems ▪ CIP-010-2 Cyber Security – Configuration Change Management and Vulnerability Assessments ▪ CIP-011-2 Cyber Security – Information Protection ▪ CIP-014-2 Physical Security

Type of Action	Specific Action or Program
	Subject to Future Enforcement ▪ NIST. DRAFT NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. 2014. ▪ NIST. Reference Architecture for Cyber-Physical Systems Project. 2016 ▪ National Futures Association's cybersecurity guidance
Coordinating and Information-Sharing Bodies	▪ Energy Government Coordinating Council (EGCC) ▪ National Infrastructure Coordinating Center (NICC) ▪ National Cybersecurity and Communications Integration Center (NCCIC) ▪ U.S. Computer Emergency Readiness Team (US-CERT) and US-CERT.gov ▪ ICS-CERT portal ▪ National Cyber Awareness System ▪ Homeland Security Information Network – Critical Infrastructure
Research and Development	▪ U.S. Department of Energy. *Roadmap to Achieve Energy Delivery Systems Cybersecurity*. 2011. ▪ U.S. Department of Homeland Security. *A Roadmap for Cybersecurity Research*. 2009. ▪ U.S. Department of Homeland Security. *Blueprint for a Secure Cyber Future Stakeholder Engagement Plan and Best Practices Report*. 2014. ▪ U.S. Department of Homeland Security. *Cybersecurity Risk Narratives of Critical Infrastructure Stakeholders*. 2014. ▪ Natural Resources Canada Smart Grid R&D projects ▪ Recovery Transformer Project
Ongoing Programs and Future Plans	▪ U.S. Department of Homeland Security. Regional Resilience Assessment Program. ▪ U.S. Department of Energy. DOE/OE commissioned work includes more than 50 projects that are developing tools and analyses to make the grid more secure and resilient to physical and cyber incidents. See Table A-2. ▪ Canada has hosted six workshops on ICS. ▪ Additional DOE-commissioned projects: - NREL. A Layered Solution to Cybersecurity. Ongoing. - SAE. Security for Plug-in Electric Vehicle Communications. Ongoing. - SAE. Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. Ongoing. - SAE. Requirements for Hardware-Protected Security for Ground Vehicle Applications. Ongoing. - INL. CAN Bus Security Across Multi-Sector Platforms. Ongoing.
Legislative	
Key Legislation	▪ Energy Policy Act of 2005 (Energy Policy Act) ▪ Fixing America's Surface Transportation (FAST) Act ▪ DOE Organization Act of 1977 ▪ Federal Energy Administration Act of 1974 ▪ Energy Supply and Environmental Coordination Act of 1974 ▪ Defense Priorities and Allocations System Program ▪ Defense Production Act of 1950 ▪ Robert T. Stafford Disaster Relief and Emergency Assistance Act ▪ Federal Power Act

Type of Action	Specific Action or Program
	▪ Emergency Management Act (Canada) ▪ Energy Supplies Emergency Act (Canada) ▪ Department of Public Safety and Emergency Preparedness Act (Canada) ▪ Emergencies Act (Canada) ▪ Canadian Security Intelligence Service Act ▪ National Energy Board Act (Canada)
Efforts Underway/ Future Plans	▪ H.R.8 – North American Energy Security and Infrastructure Act of 2015 (https://www.congress.gov/bill/114th-congress/house-bill/8) was passed by the House on 12/03/15 and has been read twice in the Senate. As of May 2016, it is with the Senate Committee on Energy and Natural Resources. It directs actions on both physical security and cybersecurity, including EMP and a plan for a strategic transformer reserve. ▪ The Energy Policy Modernization Act of 2015 (S.2012), which was reported by the Senate Committee on Energy and Natural Resources in September 2015, includes two sections primarily directed at electric grid cybersecurity, but with potential effects on physical asset protection or recovery.[445]
State/Local/Industry	
Coordinating and Information-Sharing Bodies	▪ Electricity Subsector Coordinating Council (ESCC) ▪ Energy and Utilities Sector Network (Canada) ▪ National Cross-Sector Forum (Canada) ▪ NERC Critical Infrastructure Protection Committee (CIPC) ▪ Edison Electric Institute (EEI) ▪ National Rural Electric Cooperative Association (NRECA) ▪ American Public Power Association (APPA) ▪ Canadian Electricity Association (CEA) ▪ Electricity Information Sharing and Analysis Center (E-ISAC) ▪ Cybersecurity Risk Information Sharing Program (CRISP) ▪ State and local fusion centers ▪ Information sharing and analysis organizations (ISAOs) ▪ National Governors Association (NGA) ▪ National Association of Regulatory Utility Commissioners (NARUC) ▪ National Association of State Chief Information Officers (NASCIO) ▪ Canada's Energy and Utility Regulators (CAMPUT)
Ongoing Programs and Future Plans	▪ NARUC cybersecurity initiatives ▪ NGA cybersecurity initiatives ▪ Trade association initiatives for both physical security and cybersecurity ▪ Spare Equipment Database System ▪ Spare Transformer Equipment Program (STEP) ▪ SpareConnect ▪ Grid Assurance ▪ Also see Table A-2

Table A-2: DOE Projects Addressing the Grid Security Strategy Elements

DOE Projects	Stage
Alliance Project: Convergence of Physical and Cyber Access Controls	P
Alliance Project: Cyber-Physical Security Unified Access Solution	P
Applied Resiliency for More Trustworthy Grid Operation (ARMORE)	P
ARRA Smart Grid Investment Grant Projects	P, M, R
Assessment of Susceptibility to GMD in Eastern Interconnect	M
Collaborative Defense of Transmission and Distribution Protection and Control Devices Against Cyber Attacks (CODEF)	P
Cyber-Physical Modeling and Simulation for Situational Awareness (CYMSA)	P
Cybersecurity Capability Maturity Model (C2M2)	P
Cybersecurity Intrusion Detection and Monitoring for Field Area Networks	P
Cybersecurity Procurement Language for Energy Delivery Systems (EDSs)	P
Cybersecurity Risk Information Sharing Program (CRISP)	P
Deployment of 12 Variometers in Eastern Interconnect	M
EAGLE-I	R
Emergency Support Function Leadership Group	R
Energy Incident Management Council (DOE)	R
Energy Response Team (DOE)	R
Energy Sector Security Appliances in a System for Intelligent Learning Network Configuration Management and Monitoring (Essence)	P
exe-Guard	P
Form OE-417 – Electric Emergency Incident and Disturbance Survey	R
FoxGuard Patch and Update Management Program for EDSs	P
Geomagnetic Disturbance	M
Incentive Prize Competition's Microgrid 2014 MVP Awards	M
Intrusion Detection System Sensor for Advanced Metering Infrastructure	P
Lemnos Interoperable Security	P
Microgrid Demonstrations: SPIDERS, NJ TRANSIT Grid	M
Mitigation Federal Leadership Group	M
National Electric Sector Cybersecurity Organization Resource (NESCOR)	P
National Strategy for Reducing Risk From the Loss of Large Power Transformers	P
NERC/DOE Report: High-Impact, Low-Frequency Event Risk to North American Bulk Power System	M

DOE Projects	Stage
Next-Gen Secure Scalable Communication Network for the Smart Grid	P
North American Synchrophasor Initiative (NASPI)	P, M, R
OE After-Action Event Reports and Analysis	R
Padlock	P
Practical Quantum Security for Grid Automation	P
Real-Time Application of Synchrophasors for Improving Reliability	P, M, R
Role-Based Access Control (RBAC)-Driven Least Privilege Architecture for Control Systems	P
Secure Core Component	P
Secure Information Exchange Gateway for Electric Grid Operations (SIEGate)	P
Secure Policy-Based Configuration Framework (PBCONF)	P
Secure Software Defined Radio (SDR)	P
Smart Grid Cryptographic Key Management	P
Software Defined Networking (SDN)	P
Space Weather Workshops (with government and industry partners, both foreign and domestic)	M
Strategies, Protections, and Mitigations for Electric Grid Effects From Electromagnetic Pulse	P
Supply Chain Integration for Integrity (SCI-FI)	P
Tools and Methods for Hardening Communication Security of EDSs	P
Transformer Resilience and Advanced Components Program (DOE/OE)	M
Trustworthy Cyber Infrastructure for the Power Grid (TCIPG)	P
Watchdog	P

P: Protection, M: Mitigation, R: Response

Source: U.S. Department of Energy, *Securing the United States Power Grid*, Report to Congress, May 2016, pp. 34–36.

Appendix B: Privacy and Cybersecurity

B.1. Current Data Collection and Industry General Practices

B.1.1. Smart meters

A number of privacy advocacy and consumer advocacy groups have expressed concern regarding the installation and use of smart meters.

> "Privacy and security concerns surrounding smart meter technology arise from the meters' essential functions, which include (1) recording near real-time data on consumer electricity usage; (2) transmitting this data to the smart meter using a variety of communications technologies; and (3) receiving communications from the smart meter, such as real-time energy prices or remote commands that can alter a consumer's electricity usage to facilitate demand response."[446]

> "To be useful for these purposes and many others, data recorded by smart meters must be highly detailed and, consequently, it may reveal which individual appliances a consumer is using. The data must also be transmitted to electric utilities—and possibly to third parties outside of the smart grid—subjecting it to potential interception or theft as it travels over communications networks and is stored in a variety of physical locations. These characteristics of smart meter data present privacy and security concerns that are likely to become more prevalent as government-backed initiatives expand deployment of the meters to millions of homes across the country."[447]

AMI meters form the basis of data privacy concerns. More than 40 million AMI meters have been installed across the United States, in every state and by every major type of utility.[448] Furthermore, utilities are forecasted to continue to roll-out residential AMI meters in their service territories and expand customer choices for access to their data.[449] Data collection intervals vary by utility, from 15-minute intervals to daily reads, but 1-hour intervals appear to be the norm.[450] Total kilowatt-hours (kWh) consumed over a specified period is the most common data element collected via AMI systems.[451] Data retention requirements are often set by the state public service regulatory commission.[452]

Based on present observations, utilities are not collecting data within the realm required to identify specific appliance usage—no more than 15-minute intervals and nowhere near real time. This would seem to alleviate most of consumers' privacy concerns. However, a subclass of smart meters—submeters—are intended to acquire much more detailed consumption data. Technology exists with the capability of measuring circuits or plugs at very short intervals (1 minute or less).[453] With electricity usage data collected at 1-minute intervals using a nonintrusive appliance load monitoring device, researchers from NIST were able to attribute electrical loads to specific household activities, including refrigerator cycles, washing machine use, oven use, and even kettle (boiling water) and toaster use.[454]

Generally, submeter technology companies are targeting the residential market mainly through organizations conducting research or administering energy efficiency programs and through solar power system installers.[455] Although companies have implemented platforms from which customers can access their submeter data, third parties can only receive direct access to the data if they administer the submeter program or work with a submeter user to set up automated data transfer via a programming interface.[456]

Research identifies three common submetering technology types among companies in the current market:[457]

- Plug-load outlet monitor: Appliances plug into a monitor and the monitor plugs into a wall outlet. Data is measured and recorded as electricity passes through the monitoring device as it measures the plug load of the appliance.
- Circuit-level monitor: The monitor is mounted near or within a breaker panel, using current transformers and measured or assumed voltage to determine power and energy consumption for multiple electrical circuits.
- Whole-house monitor with load disaggregation algorithms: The monitor is mounted near or within a breaker panel, using current transformers and measured line voltage to determine power and energy consumption at the electrical mains. A cloud service then uses electrical pattern detection algorithms to identify the electrical signatures of specific appliances and other loads.

Of the three submetering technology types, circuit-level monitors are the most prevalent.[458] Circuit-level monitors collect data at the circuit level (e.g., kitchen outlets, family room lights).

Further stirring privacy concerns, collected data is typically either stored on a cloud-hosted server or on internal hardware memory that may be accessed remotely via an embedded Web server.[459] Submetering technology companies have set up systems or portals to allow customers to access their own data, thereby requiring third parties to go directly to the customer in order to receive the data.[460] Some companies currently offer data access to administrators of submetering programs using their technologies.[461]

However, unlike AMI programs that span more than 500 utilities, there is significantly less activity in utility residential submetering projects.[462] Rather than through utilities, likely pathways to mass residential implementation include providing submeters as an ancillary offering with home security and/or home automation systems; providing submeters in a home builder offering; or implementing utility incentive, rebate, or demand response programs,[463] hence requiring a positive customer action before submeter installation.

At this time, there are very few submetering projects underway at utilities. Unlike regulatory involvement with utility AMI programs, there have been no regulatory initiatives or mandates to collect information at this level or interval.[464] For most utilities, technology cost recovery is dependent upon regulatory approval.[465] Technology is expensive, both to install and support, relative to AMI meters.[466] Because the technology is expensive to purchase, install, and maintain, and because there is no foreseeable regulatory or legislative mandate to install these, there is little evidence to support that submeter data will be prevalent in the near term.[467]

B.1.2 Smart meter data management

The collection of data by smart meters must be highly managed and controlled.

> "Planning for proper data interfaces of the Smart Meter System and the utility legacy systems is imperative. A software system not part of the utilities' traditional metering systems but required to operate a Smart Meter System is a Meter Data Management System (MDMS). MDMS is a major component of Smart Meter deployment and operations, and is the least understood and sometimes forgotten component of the project. This software platform receives meter data from one or multiple Smart Meter technologies, verifies and stores the data, and delivers data subsets to the utility operations applications such as billing, outage management, etc."[468]

> "An MDMS is installed and operational prior to Smart Meter deployment and is designed to meet the utilities core business needs as well as Smart Meter support. Detailed technical and business requirements, including data storage needs are developed before MDMS application selection. In addition, the data architecture and the IT infrastructure requirements are included in the requirements planning, and cannot be underestimated."[469]

> "The data system required for supporting Smart Meter deployments is determined by data requirements and number of customers. For small utilities, usually less than 100,000 customers, the Smart Meter head-end can handle the data management needs. For medium and large deployments of Smart Meters, however, the massive data and functional requirements demands a more sophisticated data management system. Interfacing to utility legacy systems is an important step in the successful operation of the system for the utility. The MDMS serves as the interface from the Smart Meter head end to the utility legacy applications to address interface issues and provide the necessary data requirements."[470]

B.2. Laws and Regulations

B.2.1. Federal

United States

> "Smart meters offer a significantly more detailed illustration of a consumer's energy usage than regular meters. Traditional meters display data on a consumer's *total* electricity usage and are typically read manually once per month. In contrast, smart meters can provide *near real-time* usage data by measuring usage electronically at a much greater frequency, such as once every 15 minutes. Current smart meter technology allows utilities to measure usage as frequently as once every minute. By examining smart meter data, it is possible to identify which appliances a consumer is using and at what times of the day, because each type of appliance generates a unique electric load signature. The National Institute of Standards and Technology wrote in 2010 that 'research

> shows that analyzing 15-minute interval aggregate household energy consumption data can by itself pinpoint the use of most major home appliances.'"[471]
>
> "Software-based algorithms would likely allow a person to extract the unique signatures of individual appliances from meter data that has been collected less frequently and is therefore less detailed."[472]
>
> "By combining appliance usage patterns, an observer could discern the behavior of occupants in a home over a period of time."[473]
>
> "General federal privacy safeguards provided under the Federal Privacy Act of 1974 protect smart meter data maintained by federal agencies, including data held by federally owned electric utilities. Section 5 of the Federal Trade Commission Act (FTC Act) allows the Federal Trade Commission (FTC) to bring enforcement proceedings against electric utilities that violate their privacy policies or fail to protect meter data from unauthorized access, provided that the FTC has statutory jurisdiction over the utilities."[474]

The Fourth Amendment of the U.S. Constitution, which establishes the parameters for government investigations, may restrict access to smart meter data or establish rules by which it can be obtained.[475] It is unclear how Fourth Amendment protection from unreasonable search and seizure would apply to smart meter data, due to the lack of cases on this issue.[476] Most of the safeguards for civil liberties and individual rights contained in the Constitution apply only to actions by state and federal governments.[477] This rule, known as the *state action doctrine*, arises when a victim claims that his or her constitutional rights have been violated, and therefore must prove that the wrongdoer had sufficient connections with the government to warrant a remedy.[478] Applying the state action test is intended to determine whether a utility's collection and dissemination of smart meter data are governed by the Fourth Amendment and, if so, to what extent.[479]

However, depending upon the manner in which smart meter services are presented to consumers, smart meter data may be protected from unauthorized disclosure or unauthorized access under the Stored Communications Act (SCA), the Computer Fraud and Abuse Act, and the Electronic Communications Privacy Act (ECPA).[480] If smart meter data is protected by these statutes, law enforcement would still appear to have the ability to access it for investigative purposes under the procedures provided in the SCA, ECPA, and the Foreign Intelligence Surveillance Act.[481] Additionally, an electric utility's privacy and security practices with regard to consumer data may be subject to Section 5 of the Federal Trade Commission (FTC) Act.[482] The FTC has recently focused its consumer protection enforcement on entities that violate their privacy policies or fail to protect data from unauthorized access.[483] This authority could apply to electric utilities in possession of smart meter data, provided that the FTC has statutory jurisdiction over them.[484] General federal privacy safeguards provided under the Federal Privacy Act of 1974 protect smart meter data maintained by federal agencies, including data held by federally owned electric utilities.[485]

Canada

> "In Canada, the provincial privacy commissioners are tasked with responding to consumer complaints regarding possible infringements to the applicable privacy law. At the heart of current Smart Grid privacy discussions is a set of core principles, which states that the consumer should have the ultimate authority over access and usage of their own energy-related data."[486]
>
> "Perhaps nowhere in Canada are these *Smart Grid Privacy Principles* more explicitly linked to the Smart Grid's architecture than in Ontario. The Ontario Information and Privacy Commissioner has set out a series of "Privacy by Design" principles for the Smart Grid. The Ontario Smart Grid Forum, an advocacy body for the development of smart grids, has formally recognized these principles as crucial to the development of the Smart Grid. Our Task Force notes that these principles broadly apply to developing Smart Grid across Canada. Legislators and regulators need to consider the precise instruments and mechanisms by which such principles should be applied and enforced."[487]

B.2.2. State

The following state legislation has been identified as it relates to data privacy and security:

- California S.B. 1476: Customer data generated by smart meters is private and can only be shared with third parties upon the consent of the customer, with the following exceptions: for basic utility purposes, at the direction of the California PUC, or to utility contractors implementing demand response, energy efficiency, or energy management programs.[488]
- Illinois S.B. 1652: Developed and implemented an advanced smart grid metering deployment plan, which included the creation of a Smart Grid Advisory Council, and H.B. 3036, which amended the smart grid infrastructure investment program and the Smart Grid Advisory Council.[489]
- Maine H.B. 563: Directed the PUC to investigate current cybersecurity and privacy issues related to smart meters.[490]
- New Hampshire S.B. 266: Prohibits utility installation of smart meters without the property owner's consent. Utilities must disclose, in writing, the installation of a smart meter.[491]
- Ohio S.B. 315: Encourages innovation and market access for cost-effective smart grid programs, and H.B. 331, which created a Cybersecurity, Education, and Economic Development Council to help improve state infrastructure for cybersecurity.[492]
- Oklahoma H.B. 1079: Established the Electronic Usage Data Protection Act that directs utilities to provide customers with access to, and protection of, smart grid consumer data.[493]
- Texas: The PUC's rules on AMI require compliance with cybersecurity standards specified by an independent meter data management organization, the regional

transmission organization, or the PUC, as well as independent security audits of investor-owned utilities that are deploying AMI.[494, 495]

- Vermont S.B. 78: Promotes statewide smart grid deployment, and S.B. 214/Act 170, which directs the public utility board to set the terms and conditions for access to wireless smart meters. This law also requires consumers' written consent prior to smart meter installation and requires the removal of smart meters upon request/cost-free opting-out of smart meters.[496]

B.3. Ongoing Efforts by Government and Industry

DOE/OE and the Federal Smart Grid Task Force have facilitated a multi-stakeholder process to develop a voluntary code of conduct (VCC) for utilities and third parties providing consumer energy use services that addresses privacy related to data enabled by smart grid technologies.[497] Industry stakeholders attended open meetings and participated in work group activities to draft the VCC principles.[498]

On September 12, 2014, DOE issued a *Federal Register* Notice announcing the availability of the draft VCC for public comment. The public comment period closed on October 14, 2014.[499] On December 11, 2014, DOE/OE, in coordination with the Federal Smart Grid Task Force, conducted a webinar to conclude the development phase of the VCC.[500] The final VCC was released on January 12, 2015.[501]

The purpose of the privacy VCC, facilitated by DOE/OE and the Federal Smart Grid Task Force, is to describe principles for voluntary adoption that:[502]

- Encourage innovation while appropriately protecting the privacy and confidentiality of customer data and providing reliable, affordable electric and energy-related services;
- Provide customers with appropriate access to their own customer data; and
- Do not infringe on or supersede any law, regulation, or governance by any applicable federal, state, or local regulatory authority.

The VCC's recommendations are intended to apply as high-level principles of conduct for both utilities and third parties.[503] However, it is envisioned that the VCC could be most beneficial to either entities that are not subject to regulation by applicable regulatory authorities, or entities whose applicable regulatory authorities have not imposed relevant requirements or guidelines.[504]

Appendix C: Endnotes

[1] U.S. Department of Energy and U.S. Department of Homeland Security, *Energy Sector-Specific Plan*, 2015, p. 27, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf.
[2] Lloyd's and the University of Cambridge, Centre for Risk Studies, *Business Blackout: The Insurance Implications of a Cyber Attack on the U.S. Power Grid*, Emerging Risk Report 2015, 2015, p. 5, http://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.
[3] The White House, Office of the Press Secretary, "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience" [Press release], 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
[4] Public Safety Canada, *National Strategy for Critical Infrastructure*, 2009, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf.
[5] North American Electric Reliability Corporation, *Understanding the Grid*, August 2013, http://www.nerc.com/news/Documents/Understanding%20the%20Grid%20DEC12.pdf.
[6] C. Miller, M. Martin, D. Pinney, and G. Walker, *Achieving a Resilient and Agile Grid*, National Rural Electric Cooperative Association, 2014, p. 2, http://www.nreca.coop/wp-content/uploads/2014/05/Achieving_a_Resilient_and_Agile_Grid.pdf.
[7] North American SynchroPhasor Initiative, *Synchrophasor System Benefits Fact Sheet*, 2010, https://www.naspi.org/File.aspx?fileID=538.
[8] U.S. Energy Information Administration, Table 1.1: Net Generation by Energy Source: Total (All Sectors), 2006 – March 2016. *Electric Power Monthly*, 2016, http://www.eia.gov/electricity/monthly/epm_table_grapher.cfm?t=epmt_1_01.
[9] North American Electric Reliability Corporation, *2013 Special Reliability Assessment: Accommodating an Increased Dependence on Natural Gas for Electric Power*, May 2013, p. 13, http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_PhaseII_FINAL.pdf.
[10] Federal Energy Regulatory Commission, Summer 2016 Energy Market and Reliability Assessment, Item No. A-3, May 19, 2016, p. 19, http://www.ferc.gov/market-oversight/reports-analyses/mkt-views/2016/05-19-16.pdf.
[11] U.S. Department of Energy and U.S. Department of Homeland Security, *Energy Sector-Specific Plan*, 2015, p. 21, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf.
[12] Federal Energy Regulatory Commission, "Electric Power Markets: National Overview," 2016, http://www.ferc.gov/market-oversight/mkt-electric/overview.asp.
[13] Federal Energy Regulatory Commission, Summer 2016 Energy Market and Reliability Assessment, Item No. A-3, May 19, 2016, pp. 17–20, http://www.ferc.gov/market-oversight/reports-analyses/mkt-views/2016/05-19-16.pdf.
[14] U.S. Department of Energy and U.S. Department of Homeland Security, *Energy Sector-Specific Plan*, 2015, pp. 19–21, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf.
[15] Kelly Ryver, "A Future Full of Drones — and the Advanced Threats They Present," *Security Intelligence,* April 29, 2016, https://securityintelligence.com/a-future-full-of-drones-and-the-advanced-threats-they-present/.
[16] Pew Research Center, "Cyber Attacks Likely to Increase," October 2014, http://www.pewInternet.org/2014/10/29/cyber-attacks-likely-to-increase/.
[17] U.S. Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team, "Mid Year Report–Incident Response," *ICS-CERT Monitor*, April/May/June 2013, p. 2, https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Apr-Jun2013.pdf.
[18] Rebecca Smith, "Utilities Seek to Stockpile Essential Parts for Disasters," *The Wall Street Journal*, April 7, 2016, http://www.wsj.com/articles/utilities-seek-to-stockpile-essential-parts-for-disasters-1460076194.

[19] U.S. Department of Homeland Security, *Considerations for a Power Transformer Emergency Spare Strategy for the Electric Utility Industry*, 2014, pp. iii and 19, https://www.dhs.gov/sites/default/files/publications/RecX%20-%20Emergency%20Spare%20Transformer%20Strategy-508.pdf.
[20] North American Electric Reliability Corporation, *Physical Security Reliability Standard Implementation*, 2015, Slide 7, https://www.midwestreliability.org/MRODocuments/CIP-014%20Guidance%20Presentation.pdf.
[21] North American Electric Reliability Corporation, *CIP Standards*, 2016, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.
[22] Deloitte, *Forward Look: Top Regulatory Trends for 2016 in Energy*, 2015, p. 8.
[23] National Institute of Standards and Technology, 2016, http://www.nist.gov/smartgrid/index.cfm.
[24] National Association of Regulatory Utility Commissioners, *Cybersecurity for State Regulators With Sample Questions for Regulators to Ask Utilities*, 2012, p. 3, http://energy.gov/sites/prod/files/NARUC%20Cybersecurity%20for%20State%20Regulators%20Primer%20-%20June%202012.pdf.
[25] New York State Ready and New York State Respond Commissions, *Summary of Recommendations & Progress Update*, 2013, p. 1, http://www.governor.ny.gov/sites/governor.ny.gov/files/archive/assets/documents/NYS-Ready-Respond-Update_10282103.pdf.
[26] U.S. Department of Energy, Testimony of Patricia A. Hoffman, Assistant Secretary for the Office of Electricity Delivery and Energy Reliability, Before the Committee on Transportation and Infrastructure, Subcommittee on Economic Development, Public Buildings, and Emergency Management, U.S. House of Representatives, April 14, 2016, p. 3, http://transportation.house.gov/uploadedfiles/2016-04-14-hoffman.pdf.
[27] U.S. Department of Energy, Testimony of Patricia A. Hoffman, Assistant Secretary for the Office of Electricity Delivery and Energy Reliability, Before the Committee on Transportation and Infrastructure, Subcommittee on Economic Development, Public Buildings, and Emergency Management, U.S. House of Representatives, April 14, 2016, pp. 3–4, http://transportation.house.gov/uploadedfiles/2016-04-14-hoffman.pdf.
[28] U.S. Department of Energy, Testimony of Patricia A. Hoffman, Assistant Secretary for the Office of Electricity Delivery and Energy Reliability, Before the Committee on Transportation and Infrastructure, Subcommittee on Economic Development, Public Buildings, and Emergency Management, U.S. House of Representatives, April 14, 2016, p. 3, http://transportation.house.gov/uploadedfiles/2016-04-14-hoffman.pdf.
[29] Lloyd's and the University of Cambridge, Centre for Risk Studies, *Business Blackout: The Insurance Implications of a Cyber Attack on the U.S. Power Grid*, Emerging Risk Report 2015, 2015, pp. 3–5, http://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.
[30] U.S. Department of Homeland Security, *Malicious Incidents Against the Electrical Sector, October 2013 – September 2014*, March 2015.
[31] U.S. Department of Homeland Security, *Malicious Incidents Against the Electrical Sector, October 2013 – September 2014*, March 2015.
[32] U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, *Year-in-Review: 2013, Energy Infrastructure Events and Expansions*, 2013, p. 10, http://www.oe.netl.DOE.gov/docs/2013-YIR-05092014.pdf.
[33] Rebecca Smith, "Assault on California Power Station Raises Alarm on Potential for Terrorism," *The Wall Street Journal*, February 5, 2014, http://www.wsj.com/articles/SB10001424052702304851104579359141941621778.

[34] "PG&E Announces Reward for Information on Metcalf Substation Attack," *Utility Dive*, April 10, 2014, http://www.utilitydive.com/press-release/20140410-pge-announces-reward-for-information-on-metcalf-substation-attack.
[35] Radio Free Europe/Radio Liberty, "Ukrainian Police Blame Second Crimean Power Outage on Sabotage," January 1, 2016, http://www.rferl.org/content/ukrainian-police-blame-second-crimean-power-outage-on-sabotage/27461403.html.
[36] Herman K. Trabish, "Arizona Substation Attacked With Bomb," *Utility Dive*, June 15, 2014, http://www.utilitydive.com/news/arizona-substation-attacked-with-bomb/274593.
[37] Tara Dodrill, "Arizona Power Grid Attacked With Homemade Bomb," *Inquistr*, June 16, 2014, http://www.inquisitr.com/1302526/arizona-power-grid-attacked.
[38] U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, *Year-in-Review: 2013, Energy Infrastructure Events and Expansions*, 2013, pp. 10-11, http://www.oe.netl.DOE.gov/docs/2013-YIR-05092014.pdf.
[39] Congressional Research Service, *Physical Security of the U.S. Power Grid: High Voltage Transformer Substations*, 2014, p. 7.
[40] Congressional Research Service, *Electric Utility Infrastructure Vulnerabilities: Transformers, Towers, and Terrorism*, 2004, p. 10, https://www.fas.org/sgp/crs/homesec/R42795.pdf.
[41] Congressional Research Service, *Electric Utility Infrastructure Vulnerabilities: Transformers, Towers, and Terrorism*, 2004, p. 18, https://www.fas.org/sgp/crs/homesec/R42795.pdf.
[42] North American Electric Reliability Corporation, *2013 Special Reliability Assessment: Accommodating an Increased Dependence on Natural Gas for Electric Power*, May 2013, p. 27, http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_PhaseII_FINAL.pdf.
[43] U.S. Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team, "Mid Year Report−Incident Response," *ICS-CERT Monitor*, April/May/June 2013, p. 2, https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Apr-Jun2013.pdf.
[44] "Attackers Ramp Up Threats to the Energy Sector," *Infosecurity Magazine*, October 30, 2013, http://www.infosecurity-magazine.com/news/attackers-ramp-up-threats-to-the-energy-sector.
[45] "Attackers Ramp Up Threats to the Energy Sector," *Infosecurity Magazine*, October 30, 2013, http://www.infosecurity-magazine.com/news/attackers-ramp-up-threats-to-the-energy-sector.
[46] "Attackers Ramp Up Threats to the Energy Sector," *Infosecurity Magazine*, October 30, 2013, http://www.infosecurity-magazine.com/news/attackers-ramp-up-threats-to-the-energy-sector.
[47] U.S. Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team, "Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)," ICS-CERT Alert No. ICS-ALERT-14-281-01E, 2014, https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.
[48] Amanda Vicinanzo, "Russian Malware 'BlackEnergy' Infiltrates US Critical Infrastructure," *Homeland Security Today*, November 13, 2014, http://www.hstoday.us/briefings/industry-news/single-article/russian-malware-blackenergy-infiltrates-us-critical-infrastructure/bb5818561feba3a1db22031626b9b8ac.html.
[49] U.S. Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team, "Cyber-Attack Against Ukrainian Critical Infrastructure," ICS-CERT Alert No. IR-ALERT-H-16-056-01, 2016, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.
[50] Heather MacKenzie, "Ukraine Power Outage Exposes Industrial Networking Risk," Belden, Inc., January 27, 2016, http://www.belden.com/blog/industrialsecurity/Ukraine-Power-Outage-Exposes-Industrial-Networking-Risk.cfm.
[51] North American Electric Reliability Corporation, Electricity Information Sharing and Analysis Center, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, 2016, pp. 8 and 20, http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.
[52] North American Electric Reliability Corporation, Electricity Information Sharing and Analysis Center, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, 2016, p. 10, http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

[53] U.S. Department of Homeland Security, *The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-based Approach Toward a Secure and Resilient Nation*, 2011, p. 1, https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf.
[54] U.S. Department of Homeland Security, *The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-based Approach Toward a Secure and Resilient Nation*, 2011, pp. 2–4, https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf.
[55] International Association of Chiefs of Police, "Awareness Brief: Homegrown Violent Extremism," http://www.theiacp.org/Portals/0/documents/HomegrownViolentExtremismAwarenessBrief.pdf.
[56] U.S. Department of Homeland Security, National Infrastructure Advisory Council, *The National Infrastructure Advisory Council's Final Report and Recommendations on the Insider Threat to Critical Infrastructures*, 2008, p. 5, https://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf.
[57] Congressional Research Service, *American Jihadist Terrorism: Combating a Complex Threat,* 2013, pp. 19-23, https://www.fas.org/sgp/crs/homesec/R42795.pdf.
[58] Congressional Research Service, *American Jihadist Terrorism: Combating a Complex Threat,* 2013, p. 1, https://www.fas.org/sgp/crs/homesec/R42795.pdf.
[59] Georgetown University Security Studies Program, National Security Critical Issue Task Force, *Report: Lone Wolf Terrorism,* 2015, p. 10, http://georgetownsecuritystudiesreview.org/wp-content/uploads/2015/08/NCITF-Final-Paper.pdf.
[60] Kelly Ryver, "A Future Full of Drones — and the Advanced Threats They Present," *Security Intelligence,* April 29, 2016, https://securityintelligence.com/a-future-full-of-drones-and-the-advanced-threats-they-present/.
[61] North American Electric Reliability Corporation and U.S. Department of Energy, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,* 2010, p. 10, http://www.nerc.com/pa/CI/Resources/Documents/HILF%20Report.pdf.
[62] U.S. Department of Homeland Security, National Infrastructure Advisory Council, *The National Infrastructure Advisory Council's Final Report and Recommendations on the Insider Threat to Critical Infrastructures*, 2008, p. 11, https://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf.
[63] U.S. Department of Homeland Security, National Infrastructure Advisory Council, *The National Infrastructure Advisory Council's Final Report and Recommendations on the Insider Threat to Critical Infrastructures*, 2008, p. 4, https://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf.
[64] U.S. Department of Homeland Security, National Infrastructure Advisory Council, *The National Infrastructure Advisory Council's Final Report and Recommendations on the Insider Threat to Critical Infrastructures*, 2008, p. 5, https://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf.
[65] U.S. Department of Homeland Security, National Infrastructure Advisory Council, *The National Infrastructure Advisory Council's Final Report and Recommendations on the Insider Threat to Critical Infrastructures*, 2008, p. 17, https://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf.
[66] U.S. Department of Homeland Security, National Infrastructure Advisory Council, *The National Infrastructure Advisory Council's Final Report and Recommendations on the Insider Threat to Critical Infrastructures*, 2008, p. 17, https://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf.
[67] U.S. Department of Homeland Security, National Infrastructure Advisory Council, *The National Infrastructure Advisory Council's Final Report and Recommendations on the Insider Threat to Critical Infrastructures*, 2008, pp. 6–9, https://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf.

[68] Choe Sang-Hun, "North Korean Missile Test Fails, South Says, Bringing String of Crashes to 3," *The New York Times*, April 28, 2016, http://www.nytimes.com/2016/04/29/world/asia/north-korea-missile-test.html.
[69] K.J. Kwon, Barbara Starr, and Jim Sciutto, "North Korea Launches Ballistic Missiles," CNN, March 18, 2016, http://www.cnn.com/2016/03/17/asia/north-korea-missile-launch/index.html.
[70] Electric Power Research Institute, *Electromagnetic Pulse (EMP) and the Power Grid*, Report No. 3002001936, 2013, http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002001936.
[71] Electric Power Research Institute, *Electromagnetic Pulse and Intentional Electromagnetic Interference (EMI) Threats to the Power Grid: Characterization of the Threat, Available Countermeasures, and Opportunities for Technology Research*, Report No. 3002000796, 2013, http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002000796.
[72] EMP Commission, *Report of the Commission to Assess the Threat to the United States From Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures*, 2008.
[73] EMP Commission, *Report of the Commission to Assess the Threat to the United States From Electromagnetic Pulse (EMP) Attack*, Volume 1: Executive Report, 2004.
[74] U.S. Department of Energy and the President's Council of Economic Advisors, *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*, 2013, p. 4, http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.
[75] New York State Ready and New York State Respond Commissions, *Summary of Recommendations & Progress Update*, 2013, http://www.governor.ny.gov/sites/governor.ny.gov/files/archive/assets/documents/NYS-Ready-Respond-Update_10282103.pdf.
[76] U.S. Department of Energy and the President's Council of Economic Advisors, *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*, 2013, http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.
[77] North American Electric Reliability Corporation and U.S. Department of Energy, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,* 2010, http://www.nerc.com/pa/CI/Resources/Documents/HILF%20Report.pdf.
[78] North American Electric Reliability Corporation, *Severe Impact Resilience: Considerations and Recommendations,* 2012, http://www.nerc.com/docs/oc/sirtf/SIRTF_Final_May_9_2012-Board_Accepted.pdf.
[79] Public Safety Canada, *A Guideline for Enhancing Canada's Critical Infrastructure Resilience to a Catastrophic Space Weather Event*, 2014.
[80] Public Safety Canada, *A Guideline for Enhancing Canada's Critical Infrastructure Resilience to a Catastrophic Earthquake*, 2013.
[81] National Science and Technology Council, *National Space Weather Action Plan*, 2015, https://www.whitehouse.gov/sites/default/files/microsites/ostp/final_nationalspaceweatheractionplan_20151028.pdf.
[82] National Science and Technology Council, *National Space Weather Strategy*, 2015, https://www.whitehouse.gov/sites/default/files/microsites/ostp/final_nationalspaceweatherstrategy_20151028.pdf.
[83] U.S. Department of Energy, *Large Power Transformers and the U.S. Electric Grid,* 2012, http://energy.gov/sites/prod/files/Large%20Power%20Transformer%20Study%20-%20June%202012_0.pdf.
[84] Congressional Research Service, *Electric Utility Infrastructure Vulnerabilities: Transformers, Towers, and Terrorism*, 2004, pp. 9–10, https://www.fas.org/sgp/crs/homesec/R42795.pdf.
[85] Conference Board of Canada, *Canada's Electricity Infrastructure: Building a Case for Investment*, April 2011, pp. i and 9, http://www.electricity.ca/media/ReportsPublications/11-257_Electricity Infrastructure[1].pdf.

[86] ICF International, *Critical Infrastructure Interdependency and Vulnerability Analysis*, August 2012.
[87] SGP Global Platts, "MISO Stakeholders Seek Solutions for Seams Issues," March 24, 2016, http://www.platts.com/latest-news/electric-power/houston/miso-stakeholders-seek-solutions-for-seams-issues-26404738.
[88] Raymond DePillo, "Seams Issues," 2013 OPSI Annual Meeting, 2013, http://www.slideserve.com/aimon/seams-issues.
[89] North American Electric Reliability Corporation, *2013 Special Reliability Assessment: Accommodating an Increased Dependence on Natural Gas for Electric Power*, May 2013, p. 83, http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_PhaseII_FINAL.pdf.
[90] North American Electric Reliability Corporation, *2013 Special Reliability Assessment: Accommodating an Increased Dependence on Natural Gas for Electric Power*, May 2013, pp. 25, 76, 85, and 87, http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_PhaseII_FINAL.pdf.
[91] U.S. Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, 2013, pp. 18–19, https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf.
[92] The White House, Office of the Press Secretary, "Presidential Policy Directive 8: National Preparedness" [Press release], 2011, https://www.dhs.gov/presidential-policy-directive-8-national-preparedness.
[93] The White House, Office of the Press Secretary, "Presidential Policy Directive 8: National Preparedness" [Press release], 2011, https://www.dhs.gov/presidential-policy-directive-8-national-preparedness.
[94] U.S. Department of Homeland Security, *National Protection Framework*, 2014, p. 10, https://www.fema.gov/media-library-data/1406717583765-996837bf788e20e977eb5079f4174240/FINAL_National_Protection_Framework_20140729.pdf.
[95] Scott Aaronson, "Assessing the Security of Critical Infrastructure: Threats, Vulnerabilities, and Solutions," Statement Before the U.S. Senate Homeland Security and Government Affairs Committee, May 18, 2016, p. 3, http://www.hsgac.senate.gov/hearings/assessing-the-security-of-critical-infrastructure-threat-vulnerabilities-and-solutions.
[96] Scott Aaronson, "Assessing the Security of Critical Infrastructure: Threats, Vulnerabilities, and Solutions," Statement Before the U.S. Senate Homeland Security and Government Affairs Committee, May 18, 2016, p. 4, http://www.hsgac.senate.gov/hearings/assessing-the-security-of-critical-infrastructure-threat-vulnerabilities-and-solutions.
[97] Scott Aaronson, "Assessing the Security of Critical Infrastructure: Threats, Vulnerabilities, and Solutions," Statement Before the U.S. Senate Homeland Security and Government Affairs Committee, May 18, 2016, p. 7, http://www.hsgac.senate.gov/hearings/assessing-the-security-of-critical-infrastructure-threat-vulnerabilities-and-solutions.
[98] Scott Aaronson, "Assessing the Security of Critical Infrastructure: Threats, Vulnerabilities, and Solutions," Statement Before the U.S. Senate Homeland Security and Government Affairs Committee, May 18, 2016, pp. 7–8, http://www.hsgac.senate.gov/hearings/assessing-the-security-of-critical-infrastructure-threat-vulnerabilities-and-solutions.
[99] U.S. Department of Homeland Security, *Considerations for a Power Transformer Emergency Spare Strategy for the Electric Utility Industry*, 2014, p. iv, https://www.dhs.gov/sites/default/files/publications/RecX%20-%20Emergency%20Spare%20Transformer%20Strategy-508.pdf.
[100] U.S. Department of Homeland Security, *Considerations for a Power Transformer Emergency Spare Strategy for the Electric Utility Industry*, 2014, p. iii, https://www.dhs.gov/sites/default/files/publications/RecX%20-%20Emergency%20Spare%20Transformer%20Strategy-508.pdf.
[101] U.S. Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, 2013, p. 14, https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf.

[102] Congressional Research Service, *Physical Security of the U.S. Power Grid: High Voltage Transformer Substations*, 2014, p. 9.
[103] North American Electric Reliability Corporation, *2013 Special Reliability Assessment: Accommodating an Increased Dependence on Natural Gas for Electric Power*, May 2013, p. 29, http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_PhaseII_FINAL.pdf.
[104] North American Electric Reliability Corporation, *2013 Special Reliability Assessment: Accommodating an Increased Dependence on Natural Gas for Electric Power*, May 2013, p. 76, http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_PhaseII_FINAL.pdf.
[105] U.S. Department of Energy and U.S. Department of Homeland Security, *Energy Sector-Specific Plan*, 2015, p. 27, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf.
[106] Edison Electric Institute, *Understanding the Electric Power Industry's Response and Restoration Process*, 2014, p. 2, http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/documents/ma_101final.pdf.
[107] Rebecca Smith, "Utilities Seek to Stockpile Essential Parts for Disasters," *The Wall Street Journal*, April 7, 2016, http://www.wsj.com/articles/utilities-seek-to-stockpile-essential-parts-for-disasters-1460076194.
[108] North American Electric Reliability Corporation, *Special Report: Spare Equipment Database System*, 2011, p. 1.
[109] Edison Electric Institute, "Spare Transformers," 2016, http://www.eei.org/ourissues/ElectricityTransmission/Pages/SpareTransformers.aspx.
[110] U.S. Department of Homeland Security, National Infrastructure Advisory Council, *The National Infrastructure Advisory Council's Final Report and Recommendations on the Insider Threat to Critical Infrastructures*, 2008, pp. 14–15, https://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf.
[111] U.S. Department of Energy and U.S. Department of Homeland Security, *Energy Sector-Specific Plan*, 2015, p. 27, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf.
[112] Information Systems Audit and Control Association, *The State of Cybersecurity, Implications for 2016: An ISACA and RSA Conference Survey*, 2016, pp. 6–7, http://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf.
[113] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 7.
[114] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 5.
[115] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 5.
[116] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 5.
[117] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 6.
[118] D. Henkin, E. Walsh, and G. Christenson, Baker Botts L.L.P., "Michigan Utility Company Hit by Ransomware: Thinking Best Practices," May 5, 2016, https://bbreaction02.bakerbotts.com/rs/vm.ashx?ct=24F76619D1E20AEDC1D180AFD72D981ED5BE7BB3D38714DD4CFF6D71424.
[119] AlgoSec, *The State of Network Security 2012: Attitudes and Opinions on the State of IT Security*, 2012, p. 5.
[120] AlgoSec, *The State of Network Security 2012: Attitudes and Opinions on the State of IT Security*, 2012, p. 5.
[121] AlgoSec, *The State of Network Security 2012: Attitudes and Opinions on the State of IT Security*, 2012, p. 5.

[122] Pew Research Center, "Cyber Attacks Likely to Increase," October 2014, http://www.pewInternet.org/2014/10/29/cyber-attacks-likely-to-increase/.
[123] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 8.
[124] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 8.
[125] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 8.
[126] U.S. Department of Homeland Security, National Infrastructure Advisory Council, *The National Infrastructure Advisory Council's Final Report and Recommendations on the Insider Threat to Critical Infrastructures*, 2008, p. 20, https://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf.
[127] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 8.
[128] GLEG, SCADA+ Pack, 2016, http://www.gleg.net/agora_scada.shtml.
[129] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 8.
[130] North American Electric Reliability Corporation, Electricity Information Sharing and Analysis Center, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, 2016, p. 5, http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.
[131] U.S. Department of Homeland Security, National Infrastructure Advisory Council, *The National Infrastructure Advisory Council's Final Report and Recommendations on the Insider Threat to Critical Infrastructures*, 2008, p. 20, https://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf.
[132] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 11.
[133] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 11.
[134] U.S. Department of Homeland Security, National Infrastructure Advisory Council, *The National Infrastructure Advisory Council's Final Report and Recommendations on the Insider Threat to Critical Infrastructures*, 2008, p. 20, https://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf.
[135] North American Electric Reliability Corporation, *CIP Standards*, 2016, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.
[136] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 1.
[137] North American Electric Reliability Corporation and U.S. Department of Energy, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,* 2010, p. 32, http://www.nerc.com/pa/CI/Resources/Documents/HILF%20Report.pdf.
[138] North American Electric Reliability Corporation and U.S. Department of Energy, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,* 2010, p. 32, http://www.nerc.com/pa/CI/Resources/Documents/HILF%20Report.pdf.
[139] D. Salmon, M. Zeller, A. Guzmán, V. Mynam, and M. Donolo, *Mitigating the Aurora Vulnerability With Existing Technology*, Schweitzer Engineering Laboratories, Inc., 2009, p. 6, https://cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6392_MitigatingAurora_MZ_20090918_Web.pdf?v=20151125-084552.
[140] D. Salmon, M. Zeller, A. Guzmán, V. Mynam, and M. Donolo, *Mitigating the Aurora Vulnerability With Existing Technology*, Schweitzer Engineering Laboratories, Inc., 2009, pp. 4–6, https://cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6392_MitigatingAurora_MZ_20090918_Web.pdf?v=20151125-084552.

[141] D. Salmon, M. Zeller, A. Guzmán, V. Mynam, and M. Donolo, *Mitigating the Aurora Vulnerability With Existing Technology*, Schweitzer Engineering Laboratories, Inc., 2009, p. 6, https://cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6392_MitigatingAurora_MZ_20090918_Web.pdf?v=20151125-084552.
[142] North American Electric Reliability Corporation and U.S. Department of Energy, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,* 2010, p. 32, http://www.nerc.com/pa/CI/Resources/Documents/HILF%20Report.pdf.
[143] North American Electric Reliability Corporation and U.S. Department of Energy, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,* 2010, p. 32, http://www.nerc.com/pa/CI/Resources/Documents/HILF%20Report.pdf.
[144] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 24.
[145] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 24.
[146] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 24.
[147] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 24.
[148] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 24.
[149] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 24.
[150] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 25.
[151] North American Electric Reliability Corporation, *CIP Standards*, 2016, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.
[152] North American Electric Reliability Corporation, Electricity Information Sharing and Analysis Center, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, 2016, p. 4, http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.
[153] North American Electric Reliability Corporation, Electricity Information Sharing and Analysis Center, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, 2016, p. 5, http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.
[154] Irfan Shakeel, "Cheating VoIP Security by Flooding the SIP," January 19, 2016, http://resources.infosecinstitute.com/cheating-voip-security-by-flooding-the-sip.
[155] T. Conway, M. Bristow, J. Doetzl, and M. Radigan, ABB Power Generation Webinar: "Lights Out in the Ukraine: Lessons Learned From a Successful Cyber Attack," n.d.
[156] National Institute of Standards and Technology, *Guidelines for Smart Grid Cyber Security,* NISTIR 7628, Revision 1, September 2014, p. 94.
[157] National Institute of Standards and Technology, *Guidelines for Smart Grid Cyber Security,* NISTIR 7628, Revision 1, September 2014, p. 102.
[158] N. Elliot, M. Molina, and D. Trombley, *A Defining Framework for Intelligent Efficiency*, American Council for an Energy-Efficient Economy, June 5, 2012.
[159] UK Centre for the Protection of National Infrastructure, Guidance, "10 Steps: Secure Configuration," updated January 16, 2015. https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets/10-steps-secure-configuration--11.
[160] Congressional Research Service, *Smart Meter Data: Privacy and Cybersecurity*, 2012, Summary.
[161] U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, "Cybersecurity," 2016, https://www.smartgrid.gov/recovery_act/overview/cyber_security.html.
[162] North American Electric Reliability Corporation and U.S. Department of Energy, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,* 2010, p. 32,

http://www.nerc.com/pa/CI/Resources/Documents/HILF%20Report.pdf.
[163] Mike Davis, "SmartGrid Device Security: Adventures in a New Medium," presented at Black Hat USA, 2009, p. 13, http://www.blackhat.com/presentations/bh-usa-09/MDAVIS/BHUSA09-Davis-AMI-SLIDES.pdf.
[164] National Renewable Energy Laboratory and the Intelligent Power and Energy Research Corporation, *Application of Bi-directional Electric Vehicle Aggregation in a Cyber Secure Microgrid Controller*, 2013, p. 1.
[165] National Renewable Energy Laboratory and the Intelligent Power and Energy Research Corporation, *Application of Bi-directional Electric Vehicle Aggregation in a Cyber Secure Microgrid Controller*, 2013, p. 2.
[166] National Renewable Energy Laboratory and the Intelligent Power and Energy Research Corporation, *Application of Bi-directional Electric Vehicle Aggregation in a Cyber Secure Microgrid Controller*, 2013, p. 4.
[167] Electric Power Research Institute, *Information and Communication Technology Program: Enabling a Smart Grid by Applying Information and Communication Technologies, 2015 Annual Review*, 2016, p. 13.
[168] Electric Power Research Institute, *Utility Cloud Integration Guidebook: A Guide for Enterprise Architects*, Technical Report, 2015, p. D-1.
[169] North American Electric Reliability Corporation and U.S. Department of Energy, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,* 2010, p. 30, http://www.nerc.com/pa/CI/Resources/Documents/HILF%20Report.pdf.
[170] North American Electric Reliability Corporation and U.S. Department of Energy, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,* 2010, p. 16, http://www.nerc.com/pa/CI/Resources/Documents/HILF%20Report.pdf.
[171] North American Electric Reliability Corporation and U.S. Department of Energy, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,* 2010, p. 30, http://www.nerc.com/pa/CI/Resources/Documents/HILF%20Report.pdf.
[172] North American Electric Reliability Corporation and U.S. Department of Energy, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,* 2010, p. 30, http://www.nerc.com/pa/CI/Resources/Documents/HILF%20Report.pdf.
[173] North American Electric Reliability Corporation and U.S. Department of Energy, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,* 2010, p. 37, http://www.nerc.com/pa/CI/Resources/Documents/HILF%20Report.pdf.
[174] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 9.
[175] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 9.
[176] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 9.
[177] Chatham House, The Royal Institute of International Affairs, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, October 5, 2015, p. 9.
[178] North American Electric Reliability Corporation and U.S. Department of Energy, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,* 2010, p. 36, http://www.nerc.com/pa/CI/Resources/Documents/HILF%20Report.pdf.
[179] North American Electric Reliability Corporation and U.S. Department of Energy, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,* 2010, p. 36, http://www.nerc.com/pa/CI/Resources/Documents/HILF%20Report.pdf.
[180] North American Electric Reliability Corporation and U.S. Department of Energy, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,* 2010, p. 36, http://www.nerc.com/pa/CI/Resources/Documents/HILF%20Report.pdf.
[181] Deloitte, *Forward Look: Top Regulatory Trends for 2016 in Energy*, 2015, p. 8.
[182] Deloitte, *Forward Look: Top Regulatory Trends for 2016 in Energy*, 2015, p. 8.
[183] Deloitte, *Forward Look: Top Regulatory Trends for 2015 in Energy*, 2014, p. 8.
[184] Deloitte, *Forward Look: Top Regulatory Trends for 2016 in Energy*, 2015, p. 8.

[185] T. Perez, B. Segalis, and D. Navetta, *Energy Cybersecurity: A Critical Concern for the Nation*, April 9, 2015, http://www.dataprotectionreport.com/2015/04/energy-cybersecurity-a-critical-concern-for-the-nation.
[186] Public Safety Canada, *A Guideline for Enhancing Canada's Critical Infrastructure Resilience to a Major Cyber Attack on the Electrical Grid and Telecommunications Systems*, n.d.
[187] Public Safety Canada, *A Guideline for Enhancing Canada's Critical Infrastructure Resilience to a Major Cyber Attack on the Electrical Grid and Telecommunications Systems*, n.d.
[188] Public Safety Canada, *A Guideline for Enhancing Canada's Critical Infrastructure Resilience to a Major Cyber Attack on the Electrical Grid and Telecommunications Systems*, n.d.
[189] Public Safety Canada, *A Guideline for Enhancing Canada's Critical Infrastructure Resilience to a Major Cyber Attack on the Electrical Grid and Telecommunications Systems*, n.d.
[190] Kenneth W. DeFontes, Jr., President and Chief Executive Officer, Baltimore Gas & Electric on Behalf of Exelon Corporation, the Edison Electric Institute, and the Electric Power Supply Association, Statement Before the House Permanent Select Committee on Intelligence, U.S. House of Representatives, February 14, 2013, p. 4.
[191] Kenneth W. DeFontes, Jr., President and Chief Executive Officer, Baltimore Gas & Electric on Behalf of Exelon Corporation, the Edison Electric Institute, and the Electric Power Supply Association, Statement Before the House Permanent Select Committee on Intelligence, U.S. House of Representatives, February 14, 2013, p. 4.
[192] Kenneth W. DeFontes, Jr., President and Chief Executive Officer, Baltimore Gas & Electric on Behalf of Exelon Corporation, the Edison Electric Institute, and the Electric Power Supply Association, Statement Before the House Permanent Select Committee on Intelligence, U.S. House of Representatives, February 14, 2013, p. 4.
[193] Kenneth W. DeFontes, Jr., President and Chief Executive Officer, Baltimore Gas & Electric on Behalf of Exelon Corporation, the Edison Electric Institute, and the Electric Power Supply Association, Statement Before the House Permanent Select Committee on Intelligence, U.S. House of Representatives, February 14, 2013, p. 4.
[194] Kenneth W. DeFontes, Jr., President and Chief Executive Officer, Baltimore Gas & Electric on Behalf of Exelon Corporation, the Edison Electric Institute, and the Electric Power Supply Association, Statement Before the House Permanent Select Committee on Intelligence, U.S. House of Representatives, February 14, 2013, p. 4.
[195] Kenneth W. DeFontes, Jr., President and Chief Executive Officer, Baltimore Gas & Electric on Behalf of Exelon Corporation, the Edison Electric Institute, and the Electric Power Supply Association, Statement Before the House Permanent Select Committee on Intelligence, U.S. House of Representatives, February 14, 2013, p. 4.
[196] Kenneth W. DeFontes, Jr., President and Chief Executive Officer, Baltimore Gas & Electric on Behalf of Exelon Corporation, the Edison Electric Institute, and the Electric Power Supply Association, Statement Before the House Permanent Select Committee on Intelligence, U.S. House of Representatives, February 14, 2013, p. 4.
[197] Kenneth W. DeFontes, Jr., President and Chief Executive Officer, Baltimore Gas & Electric on Behalf of Exelon Corporation, the Edison Electric Institute, and the Electric Power Supply Association, Statement Before the House Permanent Select Committee on Intelligence, U.S. House of Representatives, February 14, 2013, p. 4.
[198] Office of the Director of National Intelligence, U.S. Department of Homeland Security, U.S. Department of Defense, and U.S. Department of Justice, *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government Under the Cybersecurity Information Sharing Act of 2015*, February 16, 2016, https://www.us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_(103).pdf.
[199] Executive. Order No. 13691, "Promoting Private Sector Cybersecurity Information Sharing," 3 CFR, 80 FR 9349, 2015, https://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf.

[200] U.S. Department of Energy, Memo from Patricia Hoffman, Assistant Secretary, Office of Electricity Delivery and Energy Reliability, to Tom Fanning, Chairman, President, and CEO, Southern Company, and Fred Gorbet, Chairman, Board of Trustees, NERC, August 5, 2014, http://www.nerc.com/pa/CI/Resources/Documents/Department%20of%20Energy%20Letter%20-%20Cybersecurity%20Risk%20Information%20Sharing%20Program%20(CRISP).pdf.

[201] U.S. Department of Homeland Security, *Supplemental Tool: Connecting to the NICC and NCCIC*, 2013, p. 1, https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Connecting-to-the-NICC-and-NCCIC-508.pdf.

[202] U.S. Department of Homeland Security, *Supplemental Tool: Connecting to the NICC and NCCIC*, 2013, p. 1, https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Connecting-to-the-NICC-and-NCCIC-508.pdf.

[203] U.S. Department of Homeland Security, *Supplemental Tool: Connecting to the NICC and NCCIC*, 2013, p. 1, https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Connecting-to-the-NICC-and-NCCIC-508.pdf.

[204] U.S. Department of Homeland Security, *Supplemental Tool: Connecting to the NICC and NCCIC*, 2013, p. 1, https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Connecting-to-the-NICC-and-NCCIC-508.pdf.

[205] U.S. Department of Homeland Security, *Supplemental Tool: Connecting to the NICC and NCCIC*, 2013, p. 1, https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Connecting-to-the-NICC-and-NCCIC-508.pdf.

[206] U.S. Department of Homeland Security, *Supplemental Tool: Connecting to the NICC and NCCIC*, 2013, p. 2, https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Connecting-to-the-NICC-and-NCCIC-508.pdf.

[207] U.S. Department of Homeland Security, *Supplemental Tool: Connecting to the NICC and NCCIC*, 2013, p. 2, https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Connecting-to-the-NICC-and-NCCIC-508.pdf.

[208] U.S. Department of Homeland Security, *Supplemental Tool: Connecting to the NICC and NCCIC*, 2013, p. 2, https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Connecting-to-the-NICC-and-NCCIC-508.pdf.

[209] U.S. Department of Homeland Security, *Supplemental Tool: Connecting to the NICC and NCCIC*, 2013, pp. 2–3, https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Connecting-to-the-NICC-and-NCCIC-508.pdf.

[210] U.S. Department of Homeland Security, *Supplemental Tool: Connecting to the NICC and NCCIC*, 2013, p. 5, https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Connecting-to-the-NICC-and-NCCIC-508.pdf.

[211] U.S. Department of Homeland Security, *Supplemental Tool: Connecting to the NICC and NCCIC*, 2013, p. 5, https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Connecting-to-the-NICC-and-NCCIC-508.pdf.

[212] U.S. Department of Homeland Security, *Supplemental Tool: Connecting to the NICC and NCCIC*, 2013, p. 8, https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Connecting-to-the-NICC-and-NCCIC-508.pdf.

[213] National Institute of Standards and Technology, *Guidelines for Smart Grid Cyber Security,* NISTIR 7628, Revision 1, September 2014.

[214] National Institute of Standards and Technology, *Guidelines for Smart Grid Cyber Security,* NISTIR 7628, Revision 1, September 2014, p. 6.

[215] National Institute of Standards and Technology, *Guidelines for Smart Grid Cyber Security,* NISTIR 7628, Revision 1, September 2014, p. 8.

[216] National Institute of Standards and Technology, *Guidelines for Smart Grid Cyber Security,* NISTIR 7628, Revision 1, September 2014, p. 272.

[217] Edison Electric Institute, *Electric Power Industry Initiatives to Protect the Nation's Grid From Cyber Threats*, 2013, p. 1, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity%20Industry%20Initiatives.pdf.
[218] Edison Electric Institute, *Electric Power Industry Initiatives to Protect the Nation's Grid From Cyber Threats*, 2013, p. 1, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity%20Industry%20Initiatives.pdf.
[219] Edison Electric Institute, *Electric Power Industry Initiatives to Protect the Nation's Grid From Cyber Threats*, 2013, p. 1, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity%20Industry%20Initiatives.pdf.
[220] Edison Electric Institute, *Electric Power Industry Initiatives to Protect the Nation's Grid From Cyber Threats*, 2013, p. 1, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity%20Industry%20Initiatives.pdf.
[221] Edison Electric Institute, *Electric Power Industry Initiatives to Protect the Nation's Grid From Cyber Threats*, 2013, p. 1, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity%20Industry%20Initiatives.pdf.
[222] Edison Electric Institute, *Electric Power Industry Initiatives to Protect the Nation's Grid From Cyber Threats*, 2013, p. 1, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity%20Industry%20Initiatives.pdf.
[223] Edison Electric Institute, *Electric Power Industry Initiatives to Protect the Nation's Grid From Cyber Threats*, 2013, p. 1, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity%20Industry%20Initiatives.pdf.
[224] North American Electric Reliability Corporation, *Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets*, Version 1.0, 2010.
[225] North American Electric Reliability Corporation, *Grid Security Exercise, GridEx III Report*, 2016, p. iv.
[226] U.S. Department of Energy, *Securing the United States Power Grid*, Report to Congress, May 2016.
[227] U.S. Department of Homeland Security, *National Protection Framework*, 2014, pp. 27–28, https://www.fema.gov/media-library-data/1406717583765-996837bf788e20e977eb5079f4174240/FINAL_National_Protection_Framework_20140729.pdf.
[228] Edison Electric Institute, *Electric Power Industry Initiatives to Protect the Nation's Grid From Cyber Threats*, 2013, p. 2, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity%20Industry%20Initiatives.pdf.
[229] Edison Electric Institute, *Electric Power Industry Initiatives to Protect the Nation's Grid From Cyber Threats*, 2013, p. 2, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity%20Industry%20Initiatives.pdf.
[230] Edison Electric Institute, *Electric Power Industry Initiatives to Protect the Nation's Grid From Cyber Threats*, 2013, p. 2, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity%20Industry%20Initiatives.pdf.
[231] Edison Electric Institute, *Electric Power Industry Initiatives to Protect the Nation's Grid From Cyber Threats*, 2013, p. 2,

http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity%20Industry%20Initiatives.pdf.

[232] Rich Hunt, *NERC Critical Infrastructure Protection: Cyber Asset Protection*, 2008, https://www.gegridsolutions.com/smartgrid/May08/1_Cyber_Asset_Protection.pdf.

[233] U.S. Department of Homeland Security, *Cyber Security Procurement Language for Control Systems*, Version 1.8, 2008.

[234] Energy Sector Control Systems Working Group, *Cybersecurity Procurement Language for Energy Delivery Systems*, 2014.

[235] U.S. Department of Energy and the President's Council of Economic Advisors, *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*, 2013, http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.

[236] U.S. Department of Energy and the President's Council of Economic Advisors, *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*, 2013, p. 8, http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.

[237] U.S. Department of Energy and the President's Council of Economic Advisors, *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*, 2013, p. 9, http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.

[238] U.S. Department of Energy and the President's Council of Economic Advisors, *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*, 2013, p. 17, http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.

[239] Electricity Consumers Resource Council, *The Economic Impacts of the August 2003 Blackout*, 2004, pp. 1–2, http://www.elcon.org/Documents/Profiles%20and%20Publications/Economic%20Impacts%20of%20August%202003%20Blackout.pdf.

[240] U.S. Department of Energy, National Renewable Energy Laboratory, *The Value of Electricity When It's Not Available*, 2003, p. 1, http://www.nrel.gov/docs/fy03osti/34231.pdf.

[241] 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*, 2004, p. 104, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.

[242] "The Blackout: Night of Terror," *Time Magazine*, vol. 100, no. 4 (July 25, 1977): 12–36, http://content.time.com/time/subscriber/article/0,33009,919089-10,00.html.

[243] Jennifer Latson, "Why the 1977 Blackout Was One of New York's Darkest Hours," Time.com, July 13, 2015, http://time.com/3949986/1977-blackout-new-york-history.

[244] 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*, 2004, p. 104, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.

[245] 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*, 2004, p. 105, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.

[246] 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*, 2004, pp. 104–105, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.

[247] 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*, 2004, p. 18, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.

[248] Federal Energy Regulatory Commission and North American Electric Reliability Corporation, *FERC/NERC Staff Report on the September 8, 2011, Southwest Blackout Event,* 2012, p. 1, http://www.nerc.com/pa/rrm/ea/September%202011%20Southwest%20Blackout%20Event%20Document%20L/AZOutage_Report_01MAY12.pdf.

[249] 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*, 2004, p. 73, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.
[250] National Academy of Sciences, *The Electric Transmission and Distribution System as a Terrorist Target*, 2012, Chapter 1, p. 16.
[251] National Academy of Sciences, *The Electric Transmission and Distribution System as a Terrorist Target*, 2012, Chapter 3, p. 16.
[252] U.S. Department of Homeland Security, *Response Federal Interagency Operational Plan,* 2014, p. 1, http://www.fema.gov/media-library-data/1406719953589-4ab5bfa40fe82879611d945dd60230c4/Response_FIOP_FINAL_20140729.pdf.
[253] U.S. Department of Homeland Security, "Blackout! Are We Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?," Statement of W. Craig Fugate, Administrator, FEMA, Before the Committee on Transportation and Infrastructure, Subcommittee on Economic Development, Public Buildings, and Emergency Management, April 14, 2016, pp. 5–6, https://www.dhs.gov/news/2016/04/14/written-testimony-fema-administrator-house-transportation-and-infrastructure.
[254] Edison Electric Institute, *Understanding the Electric Power Industry's Response and Restoration Process*, 2014, pp. 5–6, http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/documents/ma_101final.pdf.
[255] American Public Power Association, "Mutual Aid," 2016, http://www.publicpower.org/Programs/landing.cfm?ItemNumber=38712&navItemNumber=37533.
[256] American Public Power Association, "Mutual Aid," 2016, http://www.publicpower.org/Programs/landing.cfm?ItemNumber=38712&navItemNumber=37533.
[257] National Electrical Manufacturers Association, "Smart Meters Can Reduce Power Outages and Restoration Time," 2016, https://www.nema.org/Storm-Disaster-Recovery/Smart-Grid-Solutions/Pages/Smart-Meters-Can-Reduce-Power-Outages-and-Restoration-Time.aspx.
[258] U.S. Department of Energy and the President's Council of Economic Advisors, *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*, 2013, p. 14, http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.
[259] U.S. Department of Energy and the President's Council of Economic Advisors, *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*, 2013, p. 14, http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.
[260] U.S. Department of Energy and the President's Council of Economic Advisors, *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*, 2013, p. 15, http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.
[261] U.S. Department of Energy and the President's Council of Economic Advisors, *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*, 2013, p. 17, http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.
[262] Edison Electric Institute, *Understanding the Electric Power Industry's Response and Restoration Process*, 2014, p. 4, http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/documents/ma_101final.pdf.
[263] U.S. Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team, "Malware Infections in the Control Environment," *ICS-CERT Monitor*, October/November/December 2012, https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2012.pdf.
[264] 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*, 2004, p. 109, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.
[265] U.S. Department of Homeland Security, *Emergency Support Function #12 – Energy Annex*, May 2013, p. 1, http://www.fema.gov/media-library-data/20130726-1921-25045-2193/final_esf_12_energy_20130501_r1.pdf.

[266] U.S. Department of Homeland Security, *Emergency Support Function #12 – Energy Annex*, May 2013, p. 1, http://www.fema.gov/media-library-data/20130726-1921-25045-2193/final_esf_12_energy_20130501_r1.pdf.
[267] U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, 2016, https://www.oe.netl.DOE.gov/hurricanes_emer/blackout.aspx.
[268] Public Safety Canada, *Federal Emergency Response Plan*, 2011, Annex A, p. A-6, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-rspns-pln/mrgnc-rspns-pln-eng.pdf.
[269] Public Safety Canada, *National Emergency Response System*, 2011, p. 4, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-rspns-sstm/index-eng.aspx.
[270] U.S. Department of Homeland Security, *Recovery Federal Interagency Operational Plan*, 2014, p. 2, http://www.fema.gov/media-library-data/1406719669673-6081c9249705bc59153d724abcb2e7ca/Recovery_FIOP_FINAL_20140729.pdf.
[271] New York Independent System Operator, *A Review of Distributed Energy Resources*, 2014, p. 20, http://www.nyiso.com/public/webdocs/media_room/publications_presentations/Other_Reports/Other_Reports/A_Review_of_Distributed_Energy_Resources_September_2014.pdf.
[272] "Renewables to Blunt Power Outages From Major Storms," Mass.gov, 2014, https://blog.mass.gov/energy/renewables/renewables-to-blunt-power-outages-from-major-storms.
[273] U.S. Department of Energy, Testimony of Patricia A. Hoffman, Assistant Secretary for the Office of Electricity Delivery and Energy Reliability, Before the Committee on Transportation and Infrastructure, Subcommittee on Economic Development, Public Buildings, and Emergency Management, U.S. House of Representatives, April 14, 2016, http://transportation.house.gov/uploadedfiles/2016-04-14-hoffman.pdf.
[274]U.S. Department of Energy, Department of Energy Grid Modernization Lab Call, 2015, pp. 6–7, http://www.netl.DOE.gov/File%20Library/Business/solicitations/2016GMLabCall.pdf.
[275] U.S. Department of Energy, Testimony of Patricia A. Hoffman, Assistant Secretary for the Office of Electricity Delivery and Energy Reliability, Before the Committee on Transportation and Infrastructure, Subcommittee on Economic Development, Public Buildings, and Emergency Management, U.S. House of Representatives, April 14, 2016, http://transportation.house.gov/uploadedfiles/2016-04-14-hoffman.pdf.
[276] U.S. Department of Energy, *Hardening and Resiliency, U.S. Energy Industry Response to Recent Hurricane Seasons*, 2010.
[277] U.S. Department of Energy, *Hardening and Resiliency, U.S. Energy Industry Response to Recent Hurricane Seasons*, 2010, p. 71.
[278] U.S. Department of Energy, *Hardening and Resiliency, U.S. Energy Industry Response to Recent Hurricane Seasons*, 2010, p. 72.
[279] U.S. Department of Energy, *Hardening and Resiliency, U.S. Energy Industry Response to Recent Hurricane Seasons*, 2010, p. 72.
[280] U.S. Department of Energy, *Hardening and Resiliency, U.S. Energy Industry Response to Recent Hurricane Seasons*, 2010, p. 73.
[281] U.S. Department of Energy, *Hardening and Resiliency, U.S. Energy Industry Response to Recent Hurricane Seasons*, 2010, p. 74.
[282] U.S. Department of Energy, *Hardening and Resiliency, U.S. Energy Industry Response to Recent Hurricane Seasons*, 2010, p. 43.
[283] North American Electric Reliability Corporation, *Special Report: Spare Equipment Database System*, 2011.
[284] Edison Electric Institute, "Spare Transformers," 2016, http://www.eei.org/ourissues/ElectricityTransmission/Pages/SpareTransformers.aspx.
[285] Edison Electric Institute, "Spare Transformers," 2016, http://www.eei.org/ourissues/ElectricityTransmission/Pages/SpareTransformers.aspx.
[286] Rebecca Smith, "Utilities Seek to Stockpile Essential Parts for Disasters," *The Wall Street Journal*, April 7, 2016, http://www.wsj.com/articles/utilities-seek-to-stockpile-essential-parts-for-disasters-1460076194.

[287] Paul Stockton, *Superstorm Sandy: Implications for Designing a Post-Cyber Attack Power Restoration System*, 2016, p. vii, http://www.jhuapl.edu/ourwork/nsa/papers/PostCyberAttack.pdf?utm_source=newsletter_95&utm_medium=email&utm_campaign=state-director-update-04-29-16.
[288] Paul Stockton, *Superstorm Sandy: Implications for Designing a Post-Cyber Attack Power Restoration System*, 2016, p. vii, http://www.jhuapl.edu/ourwork/nsa/papers/PostCyberAttack.pdf?utm_source=newsletter_95&utm_medium=email&utm_campaign=state-director-update-04-29-16.
[289] Paul Stockton, *Superstorm Sandy: Implications for Designing a Post-Cyber Attack Power Restoration System*, 2016, p. vii, http://www.jhuapl.edu/ourwork/nsa/papers/PostCyberAttack.pdf?utm_source=newsletter_95&utm_medium=email&utm_campaign=state-director-update-04-29-16.
[290] The White House, Office of the Press Secretary, "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience" [Press release], 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
[291] Executive Order No. 12656, "Assignment of Emergency Preparedness Responsibilities," 3 CFR, 53 FR 47491, 1988, http://www.archives.gov/federal-register/codification/executive-order/12656.html.
[292] The White House, Office of the Press Secretary, "Presidential Policy Directive 8: National Preparedness" [Press release], 2011, https://www.dhs.gov/presidential-policy-directive-8-national-preparedness.
[293] Executive Order No. 13636, "Improving Critical Infrastructure Cybersecurity," 3 CFR, 78 FR 11739, 2013, https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
[294] Executive Order No. 12656, "Assignment of Emergency Preparedness Responsibilities," 3 CFR, 53 FR 47491, 1988, Parts 1 and 2, http://www.archives.gov/federal-register/codification/executive-order/12656.html.
[295] Executive Order No. 12656, "Assignment of Emergency Preparedness Responsibilities," 3 CFR, 53 FR 47491, 1988, Section 701, http://www.archives.gov/federal-register/codification/executive-order/12656.html.
[296] Executive Order No. 12656, "Assignment of Emergency Preparedness Responsibilities," 3 CFR, 53 FR 47491, 1988, Section 702, http://www.archives.gov/federal-register/codification/executive-order/12656.html.
[297] U.S. Department of Energy and U.S. Department of Homeland Security, *Energy Sector-Specific Plan*, 2015, p. 19, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf.
[298] Executive Order No. 13603, "National Defense Resources Preparedness," 3 CFR, 77 FR 16651, 2012, Sections 201–202, https://www.gpo.gov/fdsys/pkg/FR-2012-03-22/pdf/2012-7019.pdf.
[299] Executive Order No. 13603, "National Defense Resources Preparedness," 3 CFR, 77 FR 16651, 2012, Section 203, https://www.gpo.gov/fdsys/pkg/FR-2012-03-22/pdf/2012-7019.pdf.
[300] Executive Order No. 13636, "Improving Critical Infrastructure Cybersecurity," 3 CFR, 78 FR 11739, 2013, Section 6, https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
[301] Executive Order No. 13636, "Improving Critical Infrastructure Cybersecurity," 3 CFR, 78 FR 11739, 2013, Section 8, https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
[302] Executive Order No. 13636, "Improving Critical Infrastructure Cybersecurity," 3 CFR, 78 FR 11739, 2013, Section 8, https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
[303] The White House, Office of the Press Secretary, "Presidential Policy Directive 8: National Preparedness" [Press release], 2011, Roles and Responsibilities, https://www.dhs.gov/presidential-policy-directive-8-national-preparedness.
[304] Public Law 95-91, *U.S. Department of Energy Organization Act* (91 Stat. 565; 42 USC §7101 note), 1977, http://www.usbr.gov/power/legislation/DOEorg.pdf.
[305] U.S. Congress, *Federal Energy Emergency Administration Act*, S.2776. 93rd Congress, 1974, https://www.congress.gov/bill/93rd-congress/senate-bill/2776.

[306] "Energy Supply and Environmental Coordination," 15 USC Ch. 16C, http://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter16C&edition=prelim.
[307] "Defense Priorities and Allocations System," 15 CFR 700, 15 CFR Ch. VII (1-01-12 Edition), 2012, https://www.gpo.gov/fdsys/granule/CFR-2012-title15-vol2/CFR-2012-title15-vol2-part700/content-detail.html.
[308] "Defense Priorities and Allocations System," 15 CFR 700, 15 CFR Ch. VII (1-01-12 Edition), 2012, Subpart A, Section 700.1, paragraphs (c) and (d), https://www.gpo.gov/fdsys/granule/CFR-2012-title15-vol2/CFR-2012-title15-vol2-part700/content-detail.html.
[309] "Interconnection and Coordination of Facilities; Emergencies; Transmission to Foreign Countries," 16 USC 824a, http://uscode.house.gov/view.xhtml?req=(title:16%20section:824a%20edition:prelim.
[310] U.S. Congress, *Fixing America's Surface Transportation Act*, H.R. 22, 114th Congress, 2015, Division F, Section 61001, https://www.congress.gov/bill/114th-congress/house-bill/22.
[311] U.S. Congress, *Fixing America's Surface Transportation Act*, H.R. 22, 114th Congress, 2015, Division F, Section 61003, https://www.congress.gov/bill/114th-congress/house-bill/22.
[312] U.S. Congress, *Fixing America's Surface Transportation Act*, H.R. 22, 114th Congress, 2015, Division F, Section 61002, https://www.congress.gov/bill/114th-congress/house-bill/22.
[313] U.S. Congress, *Fixing America's Surface Transportation Act*, H.R. 22, 114th Congress, 2015, Division F, Section 61005, https://www.congress.gov/bill/114th-congress/house-bill/22.
[314] Federal Energy Regulatory Commission, "About FERC," 2016, http://www.ferc.gov/about/about.asp.
[315] Federal Energy Regulatory Commission, "Federal Statutes," 2016, http://www.ferc.gov/legal/fed-sta.asp.
[316] Federal Energy Regulatory Commission, "Office of Energy Infrastructure Security (OEIS)," 2016, http://www.ferc.gov/about/offices/oeis.asp.
[317] Federal Energy Regulatory Commission, "Office of Electric Reliability (OER)," 2016, http://www.ferc.gov/about/offices/oer.asp.
[318] Executive Order No. 12656, "Assignment of Emergency Preparedness Responsibilities," 3 CFR, 53 FR 47491, 1988, Parts 1 and 2, http://www.archives.gov/federal-register/codification/executive-order/12656.html.
[319] Executive Order No. 12656, "Assignment of Emergency Preparedness Responsibilities," 3 CFR, 53 FR 47491, 1988, Section 1701, http://www.archives.gov/federal-register/codification/executive-order/12656.html.
[320] The White House, Office of the Press Secretary, "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience" [Press release], 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
[321] Executive Order No. 13636, "Improving Critical Infrastructure Cybersecurity," 3 CFR, 78 FR 11739, 2013, Section 4, https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
[322] The White House, Office of the Press Secretary, "Presidential Policy Directive 8: National Preparedness" [Press release], 2011, Roles and Responsibilities, https://www.dhs.gov/presidential-policy-directive-8-national-preparedness.
[323] U.S. Congress, *Fixing America's Surface Transportation Act*, H.R. 22, 114th Congress, 2015, https://www.congress.gov/bill/114th-congress/house-bill/22.
[324] Executive Order No. 12656, "Assignment of Emergency Preparedness Responsibilities," 3 CFR, 53 FR 47491, 1988, Parts 1 and 2, http://www.archives.gov/federal-register/codification/executive-order/12656.html.
[325] Executive Order No. 12656, "Assignment of Emergency Preparedness Responsibilities," 3 CFR, 53 FR 47491, 1988, Section 1101, http://www.archives.gov/federal-register/codification/executive-order/12656.html.
[326] Executive Order No. 12656, "Assignment of Emergency Preparedness Responsibilities," 3 CFR, 53 FR 47491, 1988, Section 1102, http://www.archives.gov/federal-register/codification/executive-order/12656.html.

[327] The White House, Office of the Press Secretary, "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience" [Press release], 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
[328] The White House, Office of the Press Secretary, "Presidential Policy Directive 8: National Preparedness" [Press release], 2011, Roles and Responsibilities, https://www.dhs.gov/presidential-policy-directive-8-national-preparedness.
[329] Executive Order No. 12656, "Assignment of Emergency Preparedness Responsibilities," 3 CFR, 53 FR 47491, 1988, Parts 1 and 2, http://www.archives.gov/federal-register/codification/executive-order/12656.html.
[330] Executive Order No. 12656, "Assignment of Emergency Preparedness Responsibilities," 3 CFR, 53 FR 47491, 1988, Section 1301, http://www.archives.gov/federal-register/codification/executive-order/12656.html.
[331] The White House, Office of the Press Secretary, "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience" [Press release], 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
[332] The White House, Office of the Press Secretary, "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience" [Press release], 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
[333] Executive Order No. 13636, "Improving Critical Infrastructure Cybersecurity," 3 CFR, 78 FR 11739, 2013, Section 7, https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
[334] The White House, Office of the Press Secretary, "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience" [Press release], 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
[335] The White House, Office of the Press Secretary, "Presidential Policy Directive 8: National Preparedness" [Press release], 2011, https://www.dhs.gov/presidential-policy-directive-8-national-preparedness.
[336] Public Safety Canada, *National Strategy for Critical Infrastructure*, 2009, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf.
[337] Government of Canada, *Emergency Management Act*, S.C. 2007, c. 15, last amended August 3, 2007, Section 3, http://laws-lois.justice.gc.ca/PDF/E-4.56.pdf.
[338] Government of Canada, *Emergency Management Act*, S.C. 2007, c. 15, last amended August 3, 2007, Section 6, http://laws-lois.justice.gc.ca/PDF/E-4.56.pdf.
[339] Public Safety Canada, *National Strategy for Critical Infrastructure*, 2009, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf.
[340] Government of Canada, *Energy Supplies Emergency Act,* R.S.C., 1985, c. E-9, last amended March 16, 2012, http://laws-lois.justice.gc.ca/PDF/E-9.pdf.
[341] Government of Canada, *Energy Supplies Emergency Act,* R.S.C., 1985, c. E-9, last amended March 16, 2012,Section 3, http://laws-lois.justice.gc.ca/PDF/E-9.pdf.
[342] Public Safety Canada, *Federal Emergency Response Plan*, 2011, Annex A, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-rspns-pln/mrgnc-rspns-pln-eng.pdf.
[343] Public Safety Canada, *Federal Emergency Response Plan*, 2011, Section 2 and Annex A, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-rspns-pln/mrgnc-rspns-pln-eng.pdf.
[344] Government of Canada, *Department of Public Safety and Emergency Preparedness Act*, S.C. 2005, c. 10 L.C., last amended February 28, 2013, http://laws-lois.justice.gc.ca/PDF/P-31.55.pdf.
[345] Government of Canada, *Emergencies Act*, R.S.C., 1985, c. 22 [4th Supp.], last amended July 2, 2003, http://laws-lois.justice.gc.ca/eng/acts/E-4.5/index.html.
[346] Government of Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*, 2010, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.
[347] Government of Canada, *Canadian Security Intelligence Service Act*, R.S.C., 1985, c. C-23, last amended June 18, 2015, http://laws-lois.justice.gc.ca/PDF/C-23.pdf.

[348] Public Safety Canada, *Federal Emergency Response Plan*, 2011, Annex A, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-rspns-pln/mrgnc-rspns-pln-eng.pdf.
[349] Defence Research and Development Canada, *Science and Technology in Action: Delivering Results for Canada's Defence and Security*, 2013, http://www.drdc-rddc.gc.ca/assets/DRDC_Internet/docs/en/ST-Strategy.pdf.
[350] Government of Canada, *National Energy Board Act*, R.S.C., 1985, c. N-7, last amended June 23, 2015, http://laws-lois.justice.gc.ca/PDF/N-7.pdf.
[351] Government of Canada, Department of Justice, "Department of Justice and Its Role in National Security," 2015, http://www.justice.gc.ca/eng/cj-jp/ns-sn/role.html.
[352] National Governors Association, "About NGA," 2015, http://www.nga.org/cms/about.
[353] Natural Resources Canada, "After the Blackout: Implementation of Mandatory Electric Reliability Standards in Canada," paper presented at the Energy and Mines Ministers' Conference, Halifax, Nova Scotia, 2015, p. 11, https://www.nrcan.gc.ca/sites/www.nrcan.gc.ca/files/www/pdf/publications/emmc/15-0137%20EMMC-After%20the%20Blackout-e.pdf.
[354] Natural Resources Canada, "After the Blackout: Implementation of Mandatory Electric Reliability Standards in Canada," paper presented at the Energy and Mines Ministers' Conference, Halifax, Nova Scotia, 2015, p. 11, https://www.nrcan.gc.ca/sites/www.nrcan.gc.ca/files/www/pdf/publications/emmc/15-0137%20EMMC-After%20the%20Blackout-e.pdf.
[355] Natural Resources Canada, "After the Blackout: Implementation of Mandatory Electric Reliability Standards in Canada," paper presented at the Energy and Mines Ministers' Conference, Halifax, Nova Scotia, 2015, p. 12, https://www.nrcan.gc.ca/sites/www.nrcan.gc.ca/files/www/pdf/publications/emmc/15-0137%20EMMC-After%20the%20Blackout-e.pdf.
[356] North American Electric Reliability Corporation, *Canadian Provincial Summaries of Standard-Making and Enforcement Functions With U.S. Comparators*, 2015, http://www.nerc.com/AboutNERC/keyplayers/Documents/Canadian%20Provincial%20Summaries%20of%20Standard-Making%20and%20Enforcement%20Functions%20with%20US%20Comparators%20(2).pdf.
[357] Canada's Energy and Utility Regulators, 2016, http://www.camput.org.
[358] North American Electric Reliability Corporation, 2016, http://www.nerc.com/Pages/default.aspx.
[359] Natural Resources Canada, "After the Blackout: Implementation of Mandatory Electric Reliability Standards in Canada," paper presented at the Energy and Mines Ministers' Conference, Halifax, Nova Scotia, 2015, p. 10, https://www.nrcan.gc.ca/sites/www.nrcan.gc.ca/files/www/pdf/publications/emmc/15-0137%20EMMC-After%20the%20Blackout-e.pdf.
[360] Electricity Subsector Coordinating Council, *Electricity Subsector Coordinating Council*, May 2016, http://www.electricitysubsector.org/ESCCBrochure.pdf.
[361] U.S. Department of Energy and U.S. Department of Homeland Security, *Energy Sector-Specific Plan*, 2015, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf.
[362] Electricity Information Sharing and Analysis Center, 2016, https://www.e-isac.com/#about.
[363] North American Transmission Forum, "About the NATF," 2016, http://www.natf.net/about/about-the-natf.
[364] Public Safety Canada, *National Strategy for Critical Infrastructure*, 2009, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf.
[365] Carleton University, Norman Paterson School of International Affairs, *Insurance and Critical Infrastructure Protection: Is There a Connection in an Environment of Terrorism?*, Canadian Centre of Intelligence and Security Studies, March 2006.

[366] U.S. Department of Energy and the Critical Infrastructure Protection Program of George Mason University School of Law, *Insurance and the Nation's Electrical Infrastructure: Mutual Understanding and Maturing Relationships*, 2005, http://cip.gmu.edu/wp-content/uploads/2013/07/CIPHS_Insurance-and-the-Nations-Electrical-Infrastructure_White-Paper.pdf.
[367] U.S. Department of Energy and the Critical Infrastructure Protection Program of George Mason University School of Law, *Insurance and the Nation's Electrical Infrastructure: Mutual Understanding and Maturing Relationships*, 2005, http://cip.gmu.edu/wp-content/uploads/2013/07/CIPHS_Insurance-and-the-Nations-Electrical-Infrastructure_White-Paper.pdf.
[368] Associated Electric and Gas Insurance Services, "About AEGIS," 2016, https://www.aegislink.com/aegislink/about_aegis.html.
[369] U.S. Department of Energy and the Critical Infrastructure Protection Program of George Mason University School of Law, *Insurance and the Nation's Electrical Infrastructure: Mutual Understanding and Maturing Relationships*, 2005, http://cip.gmu.edu/wp-content/uploads/2013/07/CIPHS_Insurance-and-the-Nations-Electrical-Infrastructure_White-Paper.pdf.
[370] U.S. Department of Energy and the Critical Infrastructure Protection Program of George Mason University School of Law, *Insurance and the Nation's Electrical Infrastructure: Mutual Understanding and Maturing Relationships*, 2005, http://cip.gmu.edu/wp-content/uploads/2013/07/CIPHS_Insurance-and-the-Nations-Electrical-Infrastructure_White-Paper.pdf.
[371] Munich Re, Hartford Steam Boiler text boxes, 2016, https://www.munichre.com/HSB/home/index.html.
[372] U.S. Government Accountability Office, *Catalogue of Federal Insurance Activities*, GAO-05-265R, March 4, 2005, http://www.gao.gov/assets/100/93046.pdf.
[373] U.S. Government Accountability Office, *Natural Disasters: Public Policy Options for Changing the Federal Role in Natural Catastrophe Insurance*, GAO-08-7, November 2007.
[374] Public Law 79-5, Ch. 20, 59 Stat. 33 codified as amended at 15 USC §§1011–1015, 1945.
[375] U.S. Government Accountability Office, "Ultimate Effects of McCarran-Ferguson Federal Antitrust Exemption on Insurer Activity Are Unclear," GAO-05-816R, July 28, 2005.
[376] U.S. Department of the Treasury, "Terrorism Risk Insurance Program," 2016, http://www.treasury.gov/resource-center/fin-mkts/Pages/program.aspx.
[377] U.S. Department of the Treasury, 31 CFR Part 50: Interim Guidance Concerning the Terrorism Risk Insurance Program Reauthorization Act of 2015, Federal Register, vol. 80, no. 25 (Friday, February 6, 2015).
https://www.gpo.gov/fdsys/pkg/FR-2015-02-06/pdf/2015-02556.pdf.
[378] Lloyd's and the University of Cambridge, Centre for Risk Studies, *Business Blackout: The Insurance Implications of a Cyber Attack on the U.S. Power Grid*, Emerging Risk Report 2015, 2015, http://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.
[379] National Association of Insurance Commissioners and the Center for Insurance Policy and Research, *Terrorism Risk Insurance Act (TRIA)*, 2015, http://www.naic.org/cipr_topics/topic_tria.htm.
[380] Congressional Research Service, *Electric Utility Infrastructure Vulnerabilities: Transformers, Towers, and Terrorism*, 2004, https://www.fas.org/sgp/crs/homesec/R42795.pdf.
[381] Federal Energy Regulatory Commission, "Commission Will Approve Applications for Prudent Cost Recovery Tied to Security Needs" [News release], 2001, https://www.ferc.gov/media/news-releases/2001/2001-3/nr01-38.PDF.
[382] Federal Energy Regulatory Commission, *FY 2005 Congressional Performance Budget Request*, 2004, http://www.ferc.gov/about/strat-docs/FY05-Budg.pdf.
[383] Congressional Research Service, *Electric Utility Infrastructure Vulnerabilities: Transformers, Towers, and Terrorism*, 2004, https://www.fas.org/sgp/crs/homesec/R42795.pdf.
[384] Federal Energy Regulatory Commission, "Reliability," 2014, http://www.ferc.gov/enforcement/reliability.asp.

[385] Federal Energy Regulatory Commission, "Reliability," 2014, http://www.ferc.gov/enforcement/reliability.asp.
[386] ScottMadden, *NERC Standards and Standards Compliance – Still a Work in Progress?*, 2008, http://www.scottmadden.com/wp-content/uploads/userFiles/misc/954b665ac4f56a089e07cd085dcbeb58.pdf.
[387] Federal Energy Regulatory Commission, *2015 Report on Enforcement*, Docket No. AD07-13-009, 2015, http://www.ferc.gov/legal/staff-reports/2015/11-19-15-enforcement.pdf.
[388] Federal Energy Regulatory Commission, *2015 Report on Enforcement*, Docket No. AD07-13-009, 2015, http://www.ferc.gov/legal/staff-reports/2015/11-19-15-enforcement.pdf.
[389] National Association of Regulatory Utility Commissioners, NARUC Ad Hoc Committee on Critical Infrastructure, *Model State Protocols for Critical Infrastructure Protection Cost Recovery*, 2004, http://pubs.naruc.org/pub/536DB639-2354-D714-51B7-FB9F46F71E3A.
[390] Congressional Research Service, *Electric Utility Infrastructure Vulnerabilities: Transformers, Towers, and Terrorism*, 2004, https://www.fas.org/sgp/crs/homesec/R42795.pdf.
[391] Congressional Research Service, *Electric Utility Infrastructure Vulnerabilities: Transformers, Towers, and Terrorism*, 2004, https://www.fas.org/sgp/crs/homesec/R42795.pdf.
[392] Evan Lehmann, "Risk: State Insurance Programs Continue to Grow Amid Hurricane Lull," *E&E News*, July 12, 2012, http://eenews.net/public/climatewire/2012/07/12/1.
[393] European Network and Information Security Agency, *Incentives and Barriers of the Cyber Insurance Market in Europe*, June 28, 2012, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurance-market-in-europe/at_download/fullReport.
[394] Insurance Information Institute, "What Does a Businessowners Policy (BOP) Cover?," 2016, http://www.iii.org/articles/what-does-a-businessowners-policy-cover.html.
[395] J.D. Harrison, "Cybersecurity Insurance: What Small Businesses Need to Know," *The Washington Post*, 2011, http://www.washingtonpost.com/blogs/on-small-business/post/cybersecurity-insurance-what-small-businesses-need-to-know/2011/12/28/gIQAYIL5MP_blog.html.
[396] Larry Ponemon, "Cost of Data Breaches Rising Globally, Says '2015 Cost of a Data Breach Study: Global Analysis'," 2015, https://securityintelligence.com/cost-of-a-data-breach-2015.
[397] Lloyd's and the University of Cambridge, Centre for Risk Studies, *Business Blackout: The Insurance Implications of a Cyber Attack on the U.S. Power Grid*, Emerging Risk Report 2015, 2015, http://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.
[398] Marsh, Academy of Risk, *Cyber Risks: Understanding Your Insurance Protection*, April 2011, http://usa.marsh.com/Portals/9/Documents/UnderstandingCyberRisks2011.pdf.
[399] Commercial Risk Europe, *Emerging Risks 2012*, 2012, http://www.agcs.allianz.com/assets/Global%20offices%20assets/UK/Documents/EMERGING%20RISKS%20REPORT%202012_low%20res.pdf.
[400] Lloyd's and the University of Cambridge, Centre for Risk Studies, *Business Blackout: The Insurance Implications of a Cyber Attack on the U.S. Power Grid*, Emerging Risk Report 2015, 2015, http://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.
[401] U.S. Department of Homeland Security, *Insurance for Cyber-Related Critical Infrastructure Loss: Key Issues*, Insurance Industry Working Session Readout Report, 2014, https://www.dhs.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session_1.pdf.
[402] Lloyd's and the University of Cambridge, Centre for Risk Studies, *Business Blackout: The Insurance Implications of a Cyber Attack on the U.S. Power Grid*, Emerging Risk Report 2015, 2015, http://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.

[403] Allianz Global Corporate and Specialty, *A Guide to Cyber Risk: Managing the Impact of Increasing Interconnectivity*, 2015, http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf.
[404] Insurance Information Institute, "U.S. Cyber Insurance Market Demonstrates Growth, Innovation in Wake of High Profile Data Breaches," 2015, http://www.iii.org/press-release/us-cyber-insurance-market-demonstrates-growth-innovation-in-wake-of-high-profile-data-breaches-102015.
[405] Allianz Global Corporate and Specialty, *A Guide to Cyber Risk: Managing the Impact of Increasing Interconnectivity*, 2015, http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf.
[406] Lloyd's and the University of Cambridge, Centre for Risk Studies, *Business Blackout: The Insurance Implications of a Cyber Attack on the U.S. Power Grid*, Emerging Risk Report 2015, 2015, http://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.
[407] re:focus partners, *Leveraging Catastrophe Bonds as a Mechanism for Resilient Infrastructure Project Finance*, 2015, http://www.refocuspartners.com/reports/RE.bound-Program-Report-December-2015.pdf.
[408] Leigh Phillips, "Cat Bonds: Cashing in on Catastrophe," June 5, 2015, http://roadtoparis.info/2014/11/18/cat-bonds-cashing-catastrophe.
[409] Leigh Phillips, "Cat Bonds: Cashing in on Catastrophe," June 5, 2015, http://roadtoparis.info/2014/11/18/cat-bonds-cashing-catastrophe.
[410] Swiss Re, *Closing the Protection Gap, Disaster Risk Financing: Smart Solutions for the Public Sector*, 2016, http://media.swissre.com/documents/Closing_the_Gap_2015_FINAL.pdf.
[411] Leigh Phillips, "Cat Bonds: Cashing in on Catastrophe," June 5, 2015, http://roadtoparis.info/2014/11/18/cat-bonds-cashing-catastrophe.
[412] Leigh Phillips, "Cat Bonds: Cashing in on Catastrophe," June 5, 2015, http://roadtoparis.info/2014/11/18/cat-bonds-cashing-catastrophe.
[413] Leigh Phillips, "Cat Bonds: Cashing in on Catastrophe," June 5, 2015, http://roadtoparis.info/2014/11/18/cat-bonds-cashing-catastrophe.
[414] Artemis, "Could the Capital Markets Solve the $1B Cyber Insurance Policy Gap?," 2015, http://www.artemis.bm/blog/2015/03/23/could-the-capital-markets-solve-the-1b-cyber-insurance-policy-gap.
[415] Artemis, "Could the Capital Markets Solve the $1B Cyber Insurance Policy Gap?," 2015, http://www.artemis.bm/blog/2015/03/23/could-the-capital-markets-solve-the-1b-cyber-insurance-policy-gap.
[416] Susanne Sclafane, "Terror Risk Bond Market Unlikely, Says Swiss Re Americas CEO, Carrier Management," 2013, http://www.carriermanagement.com/news/2013/09/19/113254.htm.
[417] Susanne Sclafane, "Terror Risk Bond Market Unlikely, Says Swiss Re Americas CEO, Carrier Management," 2013, http://www.carriermanagement.com/news/2013/09/19/113254.htm.
[418] U.S. Energy Information Administration, "What Is the Electric Power Grid and What Are Some Challenges It Faces?," December 2015, http://www.eia.gov/energy_in_brief/article/power_grid.cfm.
[419] Natural Resources Canada, "After the Blackout: Implementation of Mandatory Electric Reliability Standards in Canada," paper presented at the Energy and Mines Ministers' Conference, Halifax, Nova Scotia, 2015, https://www.nrcan.gc.ca/sites/www.nrcan.gc.ca/files/www/pdf/publications/emmc/15-0137%20EMMC-After%20the%20Blackout-e.pdf.
[420] Natural Resources Canada, "After the Blackout: Implementation of Mandatory Electric Reliability Standards in Canada," paper presented at the Energy and Mines Ministers' Conference, Halifax, Nova Scotia, 2015, pp. 5 and 10, https://www.nrcan.gc.ca/sites/www.nrcan.gc.ca/files/www/pdf/publications/emmc/15-0137%20EMMC-After%20the%20Blackout-e.pdf.
[421] Natural Resources Canada, "After the Blackout: Implementation of Mandatory Electric Reliability Standards in Canada," paper presented at the Energy and Mines Ministers' Conference, Halifax, Nova Scotia, 2015, pp. 14–15,

https://www.nrcan.gc.ca/sites/www.nrcan.gc.ca/files/www/pdf/publications/emmc/15-0137%20EMMC-After%20the%20Blackout-e.pdf.

[422] Natural Resources Canada, "After the Blackout: Implementation of Mandatory Electric Reliability Standards in Canada," paper presented at the Energy and Mines Ministers' Conference, Halifax, Nova Scotia, 2015, pp. 14–15, https://www.nrcan.gc.ca/sites/www.nrcan.gc.ca/files/www/pdf/publications/emmc/15-0137%20EMMC-After%20the%20Blackout-e.pdf.

[423] Edison Electric Institute, *Understanding the Electric Power Industry's Response and Restoration Process*, 2014, p. 6, http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/documents/ma_101final.pdf.

[424] Power-Technology.com, "The 10 Worst Blackouts of the Last 50 Years," 2015, http://www.power-technology.com/features/featurethe-10-worst-blackouts-in-the-last-50-years-4486990.

[425] Power-Technology.com, "The 10 Worst Blackouts of the Last 50 Years," 2015, http://www.power-technology.com/features/featurethe-10-worst-blackouts-in-the-last-50-years-4486990.

[426] Institute of Electrical and Electronic Engineers, Task Force on Understanding, Prediction, Mitigation, and Restoration of Cascading Failures of the IEEE Computing & Analytical Methods Subcommittee, "Mitigation and Prevention of Cascading Outages: Methodologies and Practical Applications," *Proceedings of the IEEE Power and Energy Society General Meeting*, 2013, p. 3, http://www.uvm.edu/~phines/publications/2013/cftf_2013_mitigation.pdf.

[427] Günther Beck, Dusan Povh, Dietmar Retzmann, and Erwin Teltsch, "Global Blackouts – Lessons Learned," presented at POWER-GEN Europe 2005, Milan, Italy, June 28–30, 2005, updated July 2011, p. 12, http://www.energy.siemens.com/hq/pool/hq/power-transmission/HVDC/Global_Blackouts.pdf.

[428] Günther Beck, Dusan Povh, Dietmar Retzmann, and Erwin Teltsch, "Global Blackouts – Lessons Learned," presented at POWER-GEN Europe 2005, Milan, Italy, June 28–30, 2005, updated July 2011, pp. 17 and 27, http://www.energy.siemens.com/hq/pool/hq/power-transmission/HVDC/Global_Blackouts.pdf.

[429] Institute of Electrical and Electronic Engineers, Task Force on Understanding, Prediction, Mitigation, and Restoration of Cascading Failures of the IEEE Computing & Analytical Methods Subcommittee, "Mitigation and Prevention of Cascading Outages: Methodologies and Practical Applications," *Proceedings of the IEEE Power and Energy Society General Meeting*, 2013, p. 4, http://www.uvm.edu/~phines/publications/2013/cftf_2013_mitigation.pdf.

[430] Sergey V. Buldyrev, Roni Parshani, Gerald Paul, H. Eugene Stanley, and Shlomo Havlin, "Catastrophic Cascade of Failures in Interdependent Networks," *Nature*, vol. 464 (April 15, 2010): 1025–1028, doi:10.1038/nature08932, http://polymer.bu.edu/hes/articles/bppsh10.pdf.

[431] W. Yu and M.G. Pollitt, *Does Liberalization Cause More Electricity Blackouts? Evidence From a Global Study of Newspaper Reports*, Electricity Policy Research Group Working Paper No. 0902, United Kingdom: University of Cambridge, 2009, pp. 28–29, http://www.eprg.group.cam.ac.uk/wp-content/uploads/2009/02/main-body3.pdf.

[432] W. Yu and M.G. Pollitt, *Does Liberalization Cause More Electricity Blackouts? Evidence From a Global Study of Newspaper Reports*, Electricity Policy Research Group Working Paper No. 0902, United Kingdom: University of Cambridge, 2009, p. 29, http://www.eprg.group.cam.ac.uk/wp-content/uploads/2009/02/main-body3.pdf.

[433] U.S. Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team, "Cyber-Attack Against Ukrainian Critical Infrastructure," ICS-CERT Alert No. IR-ALERT-H-16-056-01, 2016, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[434] U.S. Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team, "Cyber-Attack Against Ukrainian Critical Infrastructure," ICS-CERT Alert No. IR-ALERT-H-16-056-01, 2016, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[435] North American Electric Reliability Corporation, Electricity Information Sharing and Analysis Center, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, 2016, pp. 14–22, http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.
[436] National Academy of Sciences, *The Electric Transmission and Distribution System as a Terrorist Target*, 2012, Chapter 1, p. 14.
[437] European Regulators' Group for Electricity and Gas, *The Lessons To Be Learned From the Large Disturbance in the European Power System on the 4th of November 2006*, Reference No. E06-BAG-01-06, 2007, p. 7, http://www.energy-regulators.eu/portal/page/portal/EER_HOME/EER_PUBLICATIONS/CEER_PAPERS/Electricity/2007/E06-BAG-01-06_Blackout-FinalReport_2007-02-06.pdf.
[438] European Regulators' Group for Electricity and Gas, *The Lessons To Be Learned From the Large Disturbance in the European Power System on the 4th of November 2006*, Reference No. E06-BAG-01-06, 2007, pp. 8–11, http://www.energy-regulators.eu/portal/page/portal/EER_HOME/EER_PUBLICATIONS/CEER_PAPERS/Electricity/2007/E06-BAG-01-06_Blackout-FinalReport_2007-02-06.pdf.
[439] European Regulators' Group for Electricity and Gas, *The Lessons To Be Learned From the Large Disturbance in the European Power System on the 4th of November 2006*, Reference No. E06-BAG-01-06, 2007, p. 5, http://www.energy-regulators.eu/portal/page/portal/EER_HOME/EER_PUBLICATIONS/CEER_PAPERS/Electricity/2007/E06-BAG-01-06_Blackout-FinalReport_2007-02-06.pdf.
[440] New York State 2100 Commission, *Recommendations to Improve the Strength and Resilience of the Empire State's Infrastructure*, January 2013, p. 32, http://www.governor.ny.gov/sites/governor.ny.gov/files/archive/assets/documents/NYS2100.pdf.
[441] New York State 2100 Commission, *Recommendations to Improve the Strength and Resilience of the Empire State's Infrastructure*, January 2013, p. 80, http://www.governor.ny.gov/sites/governor.ny.gov/files/archive/assets/documents/NYS2100.pdf.
[442] New York Power Authority, *Strategic Vision 2014–2019*, 2014, https://www.nypa.gov/Strategic-Vision-Plan14-19.pdf.
[443] U.S. Department of Energy and U.S. Department of Homeland Security, *Energy Sector-Specific Plan*, 2015, p. 27, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf.
[444] Lloyd's and the University of Cambridge, Centre for Risk Studies, *Business Blackout: The Insurance Implications of a Cyber Attack on the U.S. Power Grid*, Emerging Risk Report 2015, 2015, p. 5, http://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.
[445] P.W. Parformak, *Electric Grid Physical Security: Recent Legislation*, 2016, https://www.fas.org/sgp/crs/homesec/IN10425.pdf.
[446] Congressional Research Service, *Smart Meter Data: Privacy and Cybersecurity*, 2012, p. 1.
[447] Congressional Research Service, *Smart Meter Data: Privacy and Cybersecurity*, 2012, pp. 1–2.
[448] U.S. Energy Information Administration, *An Assessment of Interval Data and Their Potential Application to Residential Electricity End-Use Modeling*, February 2015, p. 1.
[449] U.S. Energy Information Administration, *An Assessment of Interval Data and Their Potential Application to Residential Electricity End-Use Modeling*, February 2015, p. 1.
[450] U.S. Energy Information Administration, *An Assessment of Interval Data and Their Potential Application to Residential Electricity End-Use Modeling*, February 2015, p. 22.
[451] U.S. Energy Information Administration, *An Assessment of Interval Data and Their Potential Application to Residential Electricity End-Use Modeling*, February 2015, p. 22.
[452] U.S. Energy Information Administration, *An Assessment of Interval Data and Their Potential Application to Residential Electricity End-Use Modeling*, February 2015, p. 22.
[453] U.S. Energy Information Administration, *An Assessment of Interval Data and Their Potential Application to Residential Electricity End-Use Modeling*, February 2015, p. 34.

[454] Congressional Research Service, *Smart Meter Data: Privacy and Cybersecurity*, 2012, p. 5.
[455] U.S. Energy Information Administration, *An Assessment of Interval Data and Their Potential Application to Residential Electricity End-Use Modeling*, February 2015, p. 32.
[456] U.S. Energy Information Administration, *An Assessment of Interval Data and Their Potential Application to Residential Electricity End-Use Modeling*, February 2015, p. 32.
[457] U.S. Energy Information Administration, *An Assessment of Interval Data and Their Potential Application to Residential Electricity End-Use Modeling*, February 2015, p. 23.
[458] U.S. Energy Information Administration, *An Assessment of Interval Data and Their Potential Application to Residential Electricity End-Use Modeling*, February 2015, p. 24.
[459] U.S. Energy Information Administration, *An Assessment of Interval Data and Their Potential Application to Residential Electricity End-Use Modeling*, February 2015, p. 34.
[460] U.S. Energy Information Administration, *An Assessment of Interval Data and Their Potential Application to Residential Electricity End-Use Modeling*, February 2015, p. 34.
[461] U.S. Energy Information Administration, *An Assessment of Interval Data and Their Potential Application to Residential Electricity End-Use Modeling*, February 2015, p. 34.
[462] U.S. Energy Information Administration, *An Assessment of Interval Data and Their Potential Application to Residential Electricity End-Use Modeling*, February 2015, p. 23.
[463] U.S. Energy Information Administration, *An Assessment of Interval Data and Their Potential Application to Residential Electricity End-Use Modeling*, February 2015, p. 23.
[464] U.S. Energy Information Administration, *An Assessment of Interval Data and Their Potential Application to Residential Electricity End-Use Modeling*, February 2015, p. 32.
[465] U.S. Energy Information Administration, *An Assessment of Interval Data and Their Potential Application to Residential Electricity End-Use Modeling*, February 2015, p. 32.
[466] U.S. Energy Information Administration, *An Assessment of Interval Data and Their Potential Application to Residential Electricity End-Use Modeling*, February 2015, p. 34.
[467] U.S. Energy Information Administration, *An Assessment of Interval Data and Their Potential Application to Residential Electricity End-Use Modeling*, February 2015, p. 2.
[468] Edison Electric Institute and Association of Edison Illuminating Companies, *Smart Meters and Smart Meter Systems: A Metering Industry Perspective*, An EEI-AEIC-UTC White Paper, 2011.
[469] Edison Electric Institute and Association of Edison Illuminating Companies, *Smart Meters and Smart Meter Systems: A Metering Industry Perspective*, An EEI-AEIC-UTC White Paper, 2011, p. 17.
[470] Edison Electric Institute and Association of Edison Illuminating Companies, *Smart Meters and Smart Meter Systems: A Metering Industry Perspective*, An EEI-AEIC-UTC White Paper, 2011, p. 17.
[471] Congressional Research Service, *Smart Meter Data: Privacy and Cybersecurity*, 2012, p. 4.
[472] Congressional Research Service, *Smart Meter Data: Privacy and Cybersecurity*, 2012. P. 4.
[473] Congressional Research Service, *Smart Meter Data: Privacy and Cybersecurity*, 2012, p. 4.
[474] Congressional Research Service, *Smart Meter Data: Privacy and Cybersecurity*, 2012, p. 3.
[475] Congressional Research Service, *Smart Meter Data: Privacy and Cybersecurity*, 2012, p. 7.
[476] Congressional Research Service, *Smart Meter Data: Privacy and Cybersecurity*, 2012, p. 3.
[477] Congressional Research Service, *Smart Meter Data: Privacy and Cybersecurity*, 2012, p. 8.
[478] Congressional Research Service, *Smart Meter Data: Privacy and Cybersecurity*, 2012, p. 8.
[479] Congressional Research Service, *Smart Meter Data: Privacy and Cybersecurity*, 2012, p. 8.
[480] Congressional Research Service, *Smart Meter Data: Privacy and Cybersecurity*, 2012, p. 3.
[481] Congressional Research Service, *Smart Meter Data: Privacy and Cybersecurity*, 2012, p. 3.
[482] Congressional Research Service, *Smart Meter Data: Privacy and Cybersecurity*, 2012, Summary.
[483] Congressional Research Service, *Smart Meter Data: Privacy and Cybersecurity*, 2012, Summary.
[484] Congressional Research Service, *Smart Meter Data: Privacy and Cybersecurity*, 2012, Summary.
[485] Congressional Research Service, *Smart Meter Data: Privacy and Cybersecurity*, 2012, Summary.
[486] Standards Council of Canada, *The Canadian Smart Grid Standards Roadmap: A Strategic Planning Document*, 2012, p. 8.

[487] Standards Council of Canada, *The Canadian Smart Grid Standards Roadmap: A Strategic Planning Document*, 2012, p. 8.
[488] National Institute of Standards and Technology, *Guidelines for Smart Grid Cyber Security,* NISTIR 7628, Revision 1, September 2014, p. 17.
[489] National Institute of Standards and Technology, *Guidelines for Smart Grid Cyber Security,* NISTIR 7628, Revision 1, September 2014, p.17.
[490] National Institute of Standards and Technology, *Guidelines for Smart Grid Cyber Security,* NISTIR 7628, Revision 1, September 2014, p.17.
[491] National Institute of Standards and Technology, *Guidelines for Smart Grid Cyber Security,* NISTIR 7628, Revision 1, September 2014, p.18.
[492] National Institute of Standards and Technology, *Guidelines for Smart Grid Cyber Security,* NISTIR 7628, Revision 1, September 2014, p.18.
[493] National Institute of Standards and Technology, *Guidelines for Smart Grid Cyber Security,* NISTIR 7628, Revision 1, September 2014, p.18.
[494] Texas Public Utility Commission, *Order Adopting New §25.130 and Amendments to §§25.121, 25.123, 25.311, and 25.346 as approved at the Open Meeting*, May 10, 2007.
[495] Bipartisan Policy Center, Electric Grid Cybersecurity Initiative Co-chairs, *Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat*, February 2014, p. 29.
[496] National Institute of Standards and Technology, *Guidelines for Smart Grid Cyber Security,* NISTIR 7628, Revision 1, September 2014, p. 18.
[497] U.S. Department of Energy, *Data Privacy and the Smart Grid: A Voluntary Code of Conduct*, 2016, http://www.energy.gov/oe/downloads/data-privacy-and-smart-grid-voluntary-code-conduct.
[498] U.S. Department of Energy, *Data Privacy and the Smart Grid: A Voluntary Code of Conduct*, 2016, http://www.energy.gov/oe/downloads/data-privacy-and-smart-grid-voluntary-code-conduct.
[499] U.S. Department of Energy, *Data Privacy and the Smart Grid: A Voluntary Code of Conduct*, 2016, http://www.energy.gov/oe/downloads/data-privacy-and-smart-grid-voluntary-code-conduct.
[500] U.S. Department of Energy, *Data Privacy and the Smart Grid: A Voluntary Code of Conduct*, 2016, http://www.energy.gov/oe/downloads/data-privacy-and-smart-grid-voluntary-code-conduct.
[501] U.S. Department of Energy, *Data Privacy and the Smart Grid: A Voluntary Code of Conduct*, 2016, http://www.energy.gov/oe/downloads/data-privacy-and-smart-grid-voluntary-code-conduct.
[502] U.S. Department of Energy, *Data Privacy and the Smart Grid: A Voluntary Code of Conduct*, 2015, p. 1, http://www.energy.gov/sites/prod/files/2015/01/f19/VCC%20Concepts%20and%20Principles%202015_01_08%20FINAL.pdf.
[503] U.S. Department of Energy, *Data Privacy and the Smart Grid: A Voluntary Code of Conduct*, 2015, p. 1, http://www.energy.gov/sites/prod/files/2015/01/f19/VCC%20Concepts%20and%20Principles%202015_01_08%20FINAL.pdf.
[504] U.S. Department of Energy, *Data Privacy and the Smart Grid: A Voluntary Code of Conduct*, 2015, p. 1, http://www.energy.gov/sites/prod/files/2015/01/f19/VCC%20Concepts%20and%20Principles%202015_01_08%20FINAL.pdf.