Section 2(e): Assessment of Electricity Disruption Incident Response Capabilities

8/09/2017

This page intentionally left blank.

Contents

Executive Summary v
Scope and Duration of a Significant Cyber Incident vi
U.S. Readiness to Manage Consequences vii
Gap in Assets and Capabilities ix
1.0 Electric Sector Operations, Reliability, and Cybersecurity 1
1.1 An Array of Organizations Work to Provide Electricity 1
1.2 The Electric Grid Remains Reliable 2
1.3 Trends in Cybersecurity Affecting the Electric Grid 3
2.0 Scope and Duration of a Prolonged Power Outage from a Significant Cyber Incident 7
2.1 Recent DOE Analysis of Potential Cyber Incident Scenarios 7
2.2 Historical Electric Grid Impacts from All Hazards 8
2.3 A Significant Cyber Incident May Complicate Response and Restoration 10
2.4 Assessing the Impacts to the United States' National Security, Economy, and Public Health and Safety 12
2.4.1 Assessing Impacts to National Security 12
2.4.2 Assessing Impacts to the Economy 14
2.4.3 Assessing Impacts to Public Health and Safety 14
3.0 U.S. Readiness to Manage Consequences 16
3.1 Planning 16
3.1.1 *National Preparedness System* 16
3.1.2 *National Cybersecurity Incident Response Plan* 18
3.1.3 National Infrastructure Protection Plan 18
3.2 Information Sharing 19
3.3 Cyber Incident Response 19
3.3.1 Stakeholder Capabilities 20
3.4 Training and Exercises 23
3.5 Authorities that Enable Response and Recovery 23
3.6 Conclusions 25
4.0 Gap in Assets and Capabilities 26
4.1 Cyber Situational Awareness and Incident Impact Analysis 26
4.2 Roles and Responsibilities under Cyber Response Frameworks 27
4.3 Cybersecurity Integration into State Energy Assurance Planning 28
4.4 Electric Cybersecurity Workforce and Expertise 28

4.5 Supply Chain and Trusted Partners 29
4.6 Public-Private Cybersecurity Information Sharing 30
4.7 Resources for National Cybersecurity Preparedness 31
Appendix A. Cybersecurity Capabilities Catalogue for the Energy Sector 32
Functional Area: Identify 32
Functional Area: Protect 34
Functional Area: Detect 34
Functional Area: Respond 35
Functional Area: Recover 36
Appendix B. Key Resources 38
Key Authorities and References 38
National Preparedness System Resources 38
National Cyber Incident Response Plan Resources 38
National Infrastructure Security and Resilience Resources 38
Energy Sector Specific Resources 39
References in Support of Interdependent Sectors 40
Additional Resources 40
Appendix C. Endnotes 42

Executive Summary

Electricity is critical to every aspect of modern life. The United States' national security, economy, and public health and safety rely on the North American electric grid[i] every second of the day. These, and many other functions powered by the grid have likely experienced local outages caused by weather, accidents, or sometimes from tree branches falling on power lines. Larger power outages, however, are infrequent occurrences, due in part to an array of organizations that work tirelessly to ensure the grid remains reliable, resilient, and secure. Nonetheless, it is neither practical nor possible to prevent all disruptive events.[1] Grid owners and operators balance risk, investment, and cost to customers when making investments in their systems.

Cybersecurity of the U.S. electric grid has emerged as one of the most important issues facing the electricity subsector today.[2] There are key trends that are increasing the risk of significant cyber incidents.[ii] On one hand, utilities and grid operators are adopting new technologies that leverage ever-expanding amounts of data and automated control capabilities to manage the grid more efficiently and reliably. On the other hand, cyber threat actors are becoming more knowledgeable about how to exploit various aspects of the grid infrastructure, including pathways through these new technologies, to achieve their malicious objectives.[3]

As cyber capabilities become more readily available over time, state and non-state actors will continue to seek and develop techniques, tactics, and procedures[4] to use against U.S. interests.[5] It has been reported that the National Security Agency has seen intrusions into critical industrial control systems (ICS) by entities with the apparent technical capability "to take down control systems that operate U.S. power grids, water systems and other critical infrastructure."[6]

Cyberattacks and intrusions targeting U.S. electric utilities have been reported, though no lasting damage—physical, cyber-physical, or otherwise—has been observed.[7] Without precedent, it is very difficult to predict the impacts to the country of a prolonged power outage from a significant cyber incident, which remains a significant gap for the intelligence community, industry, and subject matter experts. Mitigating this gap will require detailed knowledge of the capabilities of the adversary, the real-time technical conditions of the grid and electricity markets, the behavioral responses of the operators of multiple systems and their customers, as well as tens if not hundreds of additional variables.

In both government and private industry, U.S. electricity subsector stakeholders perform regular assessments, exercises, and information sharing and coordination plans of general and specific responses to significant cyber incidents. As part of this overall coordinated effort, Executive Order 13800 on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" called for an Assessment of Electricity Disruption Incident Response Capabilities.

[i] The terms 'electric grid', 'the grid', and 'electricity system' are used interchangeably throughout this report.
[ii] Presidential Policy Directive 41 defines a significant cyber incident as a cyber incident that is (or group of related cyber incidents) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

As described in the executive order:

The Secretary of Energy and the Secretary of Homeland Security, in consultation with the Director of National Intelligence, with State, local, tribal, and territorial governments, and with others as appropriate, shall jointly assess:

> *(i) the potential scope and duration of a prolonged power outage associated with a significant cyber incident, as defined in Presidential Policy Directive 41 of July 26, 2016 (United States Cyber Incident Coordination), against the United States electric subsector;*
> *(ii) the readiness of the United States to manage the consequences of such an incident; and*
> *(iii) any gaps or shortcomings in assets or capabilities required to mitigate the consequences of such an incident.*

The assessment shall be provided to the President, through the Assistant to the President for Homeland Security and Counterterrorism, within 90 days of the date of this order, and may be classified in full or in part, as appropriate.

This assessment reflects the combined effort of the responsible departments, agencies, and partners across the United States to fulfill this requirement from the executive order.

Scope and Duration of a Significant Cyber Incident

Electric utilities, system operators, generation owners, and other electricity stakeholders have tackled resilience and reliability challenges for as long as the grid has operated. Rigorous planning ensures that the electricity system can meet the needs of customers even when equipment fails unexpectedly, whether it is due to an ice storm, a hurricane, or a significant cyber incident.[8]

Power restorations following a significant cyber incident could be more challenging than previously experienced. Despite the electricity subsector's substantial experience responding to power outages from severe weather the potentially unique characteristics of a significant cyber incident[9] may cause any electricity disruption to be larger in terms of grid impacts and customers without power and longer in duration than seen from historical events. Several factors may complicate the power sector's response and the ability of the electricity system to be restored to normal operating conditions. These factors may include: (1) no-notice events that prevent the electricity subsector from taking preemptive measures to protect the electricity system, develop restoration plans, or activate key personnel; (2) unpredictable system responses due to the potentially disparate nature of the impacts and/or the simultaneous failure of targeted critical components; (3) the additional time required to perform system diagnostics following an incident; (4) available expertise in cybersecurity, ICS, and other potentially impacted segments of grid operations; and (5) the ability of existing response mechanisms to fully support restoration due to many complicating factors.

Beyond the electricity subsector, electric outages impact the United States' national security, economy, and public health and safety.[10] To effectively assess the impacts of any power outage, it is critical to understand the complexities of the interactions between electricity and other critical infrastructures. While natural disasters can and have caused cascading failures, they are

generally contained in spatial extent, frequency, and duration; therefore, the impacts of these types of events may be more predictable than those caused by a significant cyber incident, which may be designed to target infrastructure interdependencies to create cascading failures across multiple sectors and systems.

U.S. Readiness to Manage Consequences

The United States is, in general, well prepared to manage most electricity disruptions.[iii] Efforts to secure the electric grid against cyber vulnerabilities and long-term outages primarily occur within four lines of effort: planning, information sharing, incident response, and exercises to secure the electric grid against cyber vulnerabilities and prolonged outages. Government support to industry preparedness, response, and power restoration primarily occurs within three coordination structures: the *National Preparedness System,*[11] the *National Cybersecurity Incident Response Plan,*[12] and the *National Infrastructure Protection Plan.*[13] Across these coordination structures, U.S. readiness to manage the consequences of a significant cyber event includes a cross-cutting set of capabilities:

- **Plans:** Advances in national preparedness that augment the United States' ability to respond to a power outage resulting from a significant cyber incident, including updates to *National Planning Frameworks*—the first edition of the *Protection mission area Federal Interagency Operational Plan*; the development of a *Power Outage Incident Annex* detailing federal coordination processes and approaches for managing a long-term power outage event; and *State, Local, Tribal, and Territorial (SLTT) Plans and Annexes,* including *State Energy Assurance and Emergency Response Plans* developed in most states that detail the concept of operations and resource requirements for power outage scenarios. The development of a *National Cyber Incident Response Plan*, pursuant to *Presidential Policy Directive 41*: *United States Cyber Incident Coordination*, leverages a doctrine from the *National Preparedness System* to articulate the roles and responsibilities, capabilities, and coordinating structures that support how the United States responds to and recovers from significant cyber incidents posing risks to critical infrastructure. Industry also identified organization/company specific plans to manage consequences of a power outage.

- **Information Sharing:** The United States faces complex jurisdictional challenges to electric subsector reliability and resilience that are largely untested by a significant cyber incident. Components within the electricity distribution and transmission system are owned and operated by public utilities such as federal, state, or municipal governments; consumer-owned cooperatives; or investor-owned utilities. The variation in infrastructure ownership and operation and the jurisdictional overlap add complexity to sharing actionable information in a timely manner. These complexities are compounded when information is classified or sensitive due to the limited options and access to facilitate sharing.

[iii] The rationale for this conclusion stems from the widespread recognition of the criticality of electricity infrastructure and the state and scope of efforts across the United States—including industry and government efforts—to prepare for and manage the consequences of disruptions. As elaborated in this report, there are areas where catastrophic considerations and emerging threats reveal gaps in capabilities.

- **Incident Response:** The grid operates through a distributed network of multiple entities and thousands of individuals. The ultimate responsibility for system operation and electricity restoration rests with the private sector owners and operators who collectively own much of the U.S. energy infrastructure. To ensure a secure and reliable supply of electricity, electric utilities conduct year-round preparation for all types of emergencies, including storms and other weather-related events, as well as cyber and physical infrastructure attacks. Restoration and response, as well as cross-sector coordination to manage industry continuity, require both industry and government capabilities. Sector responses identified several incident response capabilities, including cybersecurity tools and resources, backup power generation, and mutual aid agreements.

- **Training and Exercises**: The national preparedness community—including SLTT governments, the federal government, and industry partners—regularly conduct exercises to practice energy restoration activities. Training is an important component of the exercise process. Cyber response training that includes the unique knowledge of electrical grid operation and ICS should be more prevalent to develop the workforce necessary to prepare for a significant cyber incident impacting the grid.

Gap in Assets and Capabilities

Considering the potential impact of a significant cyber event and the state of preparedness for responding to potential events, this assessment enumerates gaps in capabilities and capacity that exist around enhancing cyber incident response capacity, developing high-priority plans, augmenting scarce and critical resources, and understanding and characterizing response efforts to catastrophic incidents. The gaps highlighted in sector responses are organized under the following categories:

1. **Cyber Situational Awareness and Incident Impact Analysis:** Existing capabilities for assessing potential consequences and impacts from cyber-related disruptions and for sharing relevant situational awareness in a timely, coordinated manner across sectors are often unable to provide the detail needed to better inform government executives, regulators, and utilities of potential risks (particularly with long-term events).

2. **Roles and Responsibilities under Cyber Response Frameworks:** Whole community partners commonly request further clarity on the roles and responsibilities in responding to a cyber incident under the *National Preparedness System*.

3. **Cybersecurity Integration into State Energy Assurance Planning:** There are gaps in incorporating cybersecurity concerns, including planning for long-term disruption events, into state emergency response and energy assurance planning.

4. **Electric Cybersecurity Workforce and Expertise:** The electric subsector faces challenges in recruiting and maintaining cybersecurity experts with strong knowledge of cybersecurity practices and the requisite knowledge of ICS used to operate the electric grid.

5. **Supply Chain and Trusted Partners:** Additional efforts are needed to facilitate further integration of cybersecurity across the electricity supply chain. This includes human resource considerations to protect against insider threats, as well as efforts to include cyber consideration into up-front areas of electric grid development through system design processes and system architectures.

6. **Public-Private Cybersecurity Information Sharing:** Stakeholders have noted that a continued challenge for the electricity subsector is the ability of all whole community partners to ensure effective cybersecurity information sharing through the bi-directional flow of information and intelligence between industry and government.

7. **Resources for National Cybersecurity Preparedness:** There are many resources and tools available to utilities to improve response efforts; however, these resources and their applicability are not always well coordinated or understood among various cross-sector partners.

1.0 Electric Sector Operations, Reliability, and Cybersecurity

The North American electric grid[i] has been consistently reliable despite numerous risks and hazards. As the grid changes over the coming years understanding what can be done to maintain resilience in a variety of conditions will be important to maintaining reliability. Rigorous planning ensures that the electricity system can meet the needs of customers, even when equipment fails unexpectedly. New cybersecurity risks are emerging as the electric grid becomes increasingly dependent on automation technology and as cyber adversaries continue to demonstrate their interests and capabilities to access these, and other, infrastructure critical to grid operations.

1.1 An Array of Organizations Work to Provide Electricity

The electric grid in North America is designed and operated to recover from any disruption, whether from a hurricane or cyber incident. The grid is made up of a vast network of controls and equipment needed to generate, transmit, and distribute electricity. The bulk power system is composed of four distinct transmission networks, also called interconnections.[1] This design prevents power loss on one grid from affecting the other three, as the interconnections are electrically independent from each other, except for a few direct current (DC) links. Additional design features at both the distribution and transmission levels of the grid defend against cascading failures, including those that allow segments of the grid to separate to prevent system disturbances from spreading.

Operating the grid is an enormously complex technical challenge. An array of organizations that operate across multiple jurisdictions perform real-time and long-term assessments of the grid's resources and conditions to instantaneously balance electricity supply and demand for millions of customers. These include investor-owned utilities, publicly owned utilities and cooperatives, as well as regional oversight entities, called regional transmission organizations (RTOs) and independent system operators (ISOs). These non-profit organizations ensure reliability and optimize supply and demand bids for wholesale electric power.

A mix of public and private organizations monitor the bulk power system, assess resource adequacy (i.e., determine if there is enough generation and transmission capacity), assess the emergency preparedness of operators and users, and develop and enforce reliability standards, including those related to cybersecurity.[2] The Energy Policy Act of 2005 created the Electric Reliability Organization (ERO), an independent, self-regulating entity that enforces mandatory electric reliability rules on all users, owners, and operators of the U.S. transmission system. In July 2006, the Federal Energy Regulatory Commission (FERC) certified the North American Electric Reliability Corporation (NERC) as the ERO.[3] Currently, there are more than 100 standards, with more than 1,300 requirements applicable and mandatory in the United States.[4] These standards are used for planning and operations and are an integral part of ensuring grid reliability.

[i] The terms 'electric grid', 'the grid', and 'electricity system' are used interchangeably throughout this report.

1.2 The Electric Grid Remains Reliable

Electric utilities, system operators, generation owners, and other electricity stakeholders have tackled resilience and reliability challenges for as long as the grid has operated. Large outages are infrequent because system owners and operators responsibly practice "defense in depth," meaning that they protect the bulk power system through layers of safety-related practices and equipment. These include developing rigorous design standards;[ii] conducting planning and operations studies, including contingency plans to ensure the grid serves customers even when equipment fails unexpectedly; as well as maintaining surplus generation and transmission capacity and backup capabilities for critical functions.[5] These practices are crucial to maintaining system operations during any type of disruption, whether it is due to an ice storm, a hurricane, or a significant cyber incident.

There are two principal components to bulk power system reliability: resource adequacy and transmission security. Adequacy means having sufficient resources to provide customers with a continuous supply of electricity at the proper voltage and frequency, virtually all the time. Security means the ability for the electricity system to withstand sudden, unexpected disturbances ranging from short circuits to cyber incidents.

Studying the performance of transmission and generation sources on the grid shows consistent performance over the years. One measure of performance, developed by NERC, is the Severity Risk Index, which indicates the stress on the bulk power system.[6] As shown in **Figure 1**, the relatively smooth slopes indicate that the grid has performed rather consistently. For the 10 events in 2016 with the greatest impacts, most of which were due to severe weather, none resulted in significant stress to the grid.[iii]

[ii] Including, but not limited to, improvements in the National Electrical Safety Code, The Institute of Electrical and Electronics Engineers Standards, and American Society for Civil Engineers Standards which have aided in the resilient design of systems to various natural and man-made hazards.

[iii] The SRI is calculated from three sets of weighted components. 1) Transmission system automatic outages for voltages 200 kV+, 2) Generation system unplanned outages, and 3) Distribution load lost as a result of events upstream of the distribution system

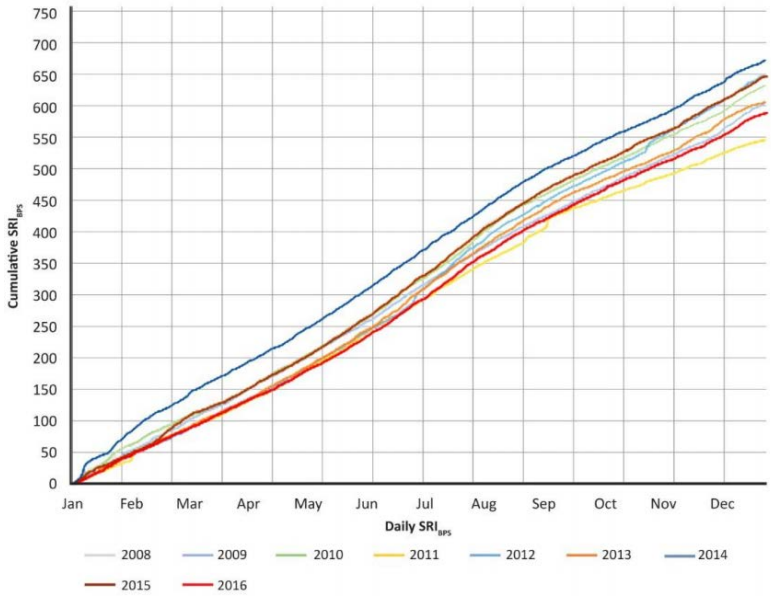

Figure 1. NERC Annual Bulk Power System Cumulative Severity Risk Index[7]

The distribution level of the grid experiences the most outages, in part due to the vastness of the poles, wires, substations, and other components located throughout the country. While multiple metrics are widely used to understand the performance of electric utilities, the System Average Interruption Duration Index (SAIDI) is one that measures the total duration of an interruption for the average customer given a defined time period. According to one survey of 96 electric utilities in North America, in 2015, the median outage duration for the average customer was 115 minutes, a level that has declined steadily from the 2005 value of 145 minutes.[8]

To maintain grid reliability and resilience, utilities have adopted new technologies. Industrial control systems (ICS) control most of the mechanical operations in power plants, substations, and other power system equipment. ICS have added new functionalities to provide utilities with more situational awareness and management capabilities by using new communication and network technologies, among others.[9] However, many of these advances, which utilize two-way flows, automation, and centralized controls, have resulted in new vulnerabilities related to cybersecurity, even as utilities adopt increasing levels of protection for their businesses and operations networks.[10]

1.3 Trends in Cybersecurity Affecting the Electric Grid

Electric grid cybersecurity has emerged as one of the most important issues facing the electricity subsector today. According to NERC, cyber vulnerabilities remain a high-risk profile relative to grid reliability.[11] A primary area of concern is the ICS that manage the operations of significant aspects of the grid and have played a key role in assisting utilities in delivering reliable power to customers. Since 2001, more than 1,000 publicly known ICS vulnerabilities have been discovered, reported, and fixed.[12]

Based on the number of reported incidents,[iv] from energy sector participants, to the Department of Homeland Security's (DHS') Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)—the U.S. energy sector, which includes the oil, natural gas, and electricity subsectors, is one of the most highly targeted critical infrastructure sectors (**Figure 2**).[13]

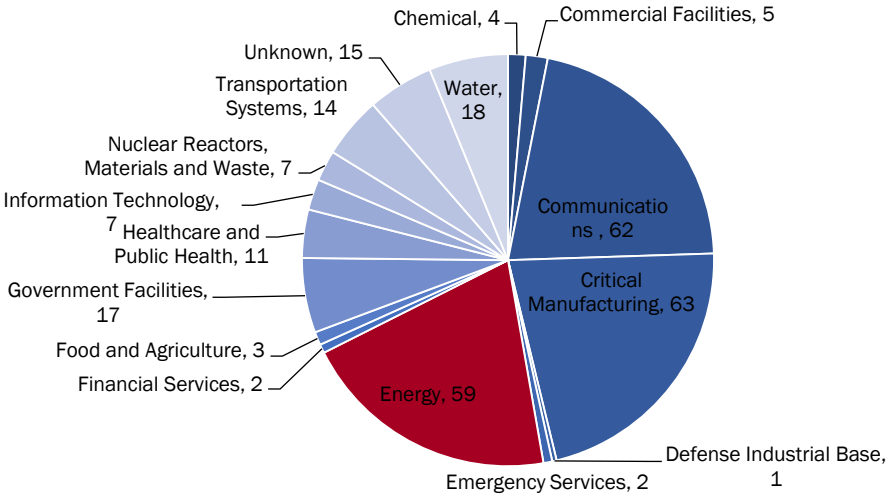

Figure 2. Reported Cyber Incidents by Critical Infrastructure Sectors, 2016[14]

Cyber adversaries have become more knowledgeable about how to exploit ICS.[15] Public examples of attacks on foreign ICS demonstrate that attackers may commandeer ICS to issue valid commands, leveraging technical knowledge about system operations to ensure that controls perform specific functions at specific times to create a desired impact to electric grids (See Text Box 1). Threat actors—including nation-states, non-state groups, or individual actors—can acquire or develop capabilities through multiple means, such as purchasing destructive malware and other capabilities or paying experts to search for vulnerabilities and develop exploits. This practice has created a market that serves multiple actors, often for competing purposes. As cyber capabilities become more readily available over time, state and non-state actors will continue to seek and develop cyber capabilities to use against U.S. interests.[16]

Each utility must conduct an analysis and deploy its own appropriate mitigations to protect its uniquely designed information technology (IT) and operational technology (OT) networks from a range of adversaries. **Figure 3** describes some possible attack vectors for an electric utility's business and operations networks.

[iv] ICS-CERT notes that its established partnerships with energy sector participants (to include electricity, oil, and natural gas) contributes to the number of incident reports the organization receives, in comparison to other critical infrastructure sectors

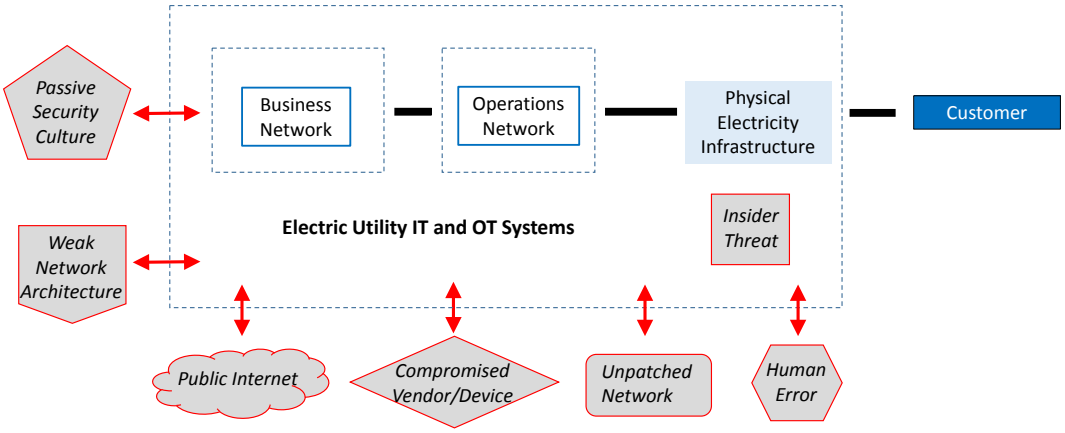

Figure 3. Example Cyberattack Vectors for an Electric Utility

As the electricity system grows in intelligence, cybersecurity must encompass not only utility-owned systems, but some aspects of customer and third-party components that interact with the grid, such as advanced meters and devices behind the meter. Cybersecurity is critically important as a function of networks, software, data, and the networks that use data to keep the electricity system operating. Finally, there are human elements to cybersecurity, including system operators, customers, and threat actors interacting at all levels of a system. With such a dynamic and broad environment to consider, cybersecurity for the electricity subsector cannot be a stagnant prescription; it must continue to evolve along with the rapid evolution of technology, threats, and vulnerabilities.

Text Box 1. Case Study: Ukraine Cyber Attack

On December 23, 2015, three Ukrainian electricity distribution companies suffered widespread power outages due to a cyberattack. The first known cyber-enabled disruption of electricity service, the attacks were executed within 30 minutes of each other and resulted in outages for 225,000 customers for 1–6 hours. *Note that an investigation is underway regarding a second attack on Ukraine's power grid that resulted in parts of the capital, Kiev, without power in late December 2016.*

The attackers hijacked distribution-level industrial control systems (ICS) and issued commands through the Human Machine Interface (HMI) that resulted in power outages. Meanwhile, the attackers locked out the grid operators to diminish the operators' ability to override the attack.

Reconnaissance: The attackers studied Ukraine's electricity and related systems for at least 6 months. A variety of open-source information was available to the attackers on the technology used by the Ukrainian distribution companies. For example, a detailed list was found online of the types and versions of Ukraine's remote terminal units, which interface between the control networks and systems. The attackers discovered that the virtual private network (VPN) between the business network and the ICS lacked two-factor authentication and that the firewall featured remote access for certain credentials.

Spear Phishing: Based on the reconnaissance, the attackers targeted specific employees in specific components of the distribution companies with a spear-phishing campaign. For months, these emails, which contained corrupted Microsoft Word files, were sent to specific information technology staff and system administrators at multiple organizations in Ukraine, including many of the distribution companies. When the documents were opened, a pop-up encouraged users to enable macros, which started installing the BlackEnergy3 malware.

BlackEnergy3: The malware allowed the attackers to communicate with the infected system. The attackers soon began harvesting credentials and escalating their privileges, while establishing persistent access to the targeted systems. This included identifying avenues between the business and the ICS networks, such as the weaknesses in the VPNs. The attackers took over the supervisory control and data acquisition HMI to open the circuit breakers and enable a cascading failure of large portions of the grid. At least 27 substations were taken offline across the three energy companies, impacting roughly 225,000 customers. In at least one distribution company, the attackers discovered a network connected to an uninterruptible power supply (UPS). The UPS, which was supporting the control centers and data centers, was taken offline to diminish the operators' view of the network and limit forensic discovery after the event. **BlackEnergy3 malware has also been found within organizations that operate critical infrastructure in the United States and in partner nations.** Utilities across the world rely on the same technology and systems, which makes it easier for attackers to develop targeted capabilities.

KillDisk: Malicious firmware was uploaded to lock out the grid operators and ensure that, once recovered, the operators could not issue remote commands to the substations.

Key Industry Sources:

- SANS ICS, Electricity Information Sharing and Analysis Center, *TLP: White Analysis of the Cyber Attack on the Ukrainian Power Grid, Defense Use Case* (Washington, DC: E-ISAC, March 18, 2016). https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
- Department of Homeland Security, "Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure," https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

2.0 Scope and Duration of a Prolonged Power Outage from a Significant Cyber Incident

Executive Order 13800 on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" directed the Secretary of Energy and the Secretary of Homeland Security to assess the potential scope and duration of a prolonged power outage associated with a significant cyber incident as defined by *Presidential Policy Directive 41* (PPD-41): *United States Cyber Incident Coordination*. [17]

Following a significant cyber incident, power restoration could be more challenging than previously experienced. Based on the electricity subsector's performance during prior power outages and the potentially unique characteristics of a significant cyber incident, the disruption may be larger in terms of grid impacts and customers without power for longer time periods than seen historically. The potential impacts to national security, the economy, and public health and safety could also be larger due to many complicating factors. However, as discussed in Section 1, grid operators prepare for unexpected equipment failures and have efforts in place to prepare for, respond to, and recover from cyber incidents.[18]

2.1 Recent DOE Analysis of Potential Cyber Incident Scenarios

A significant cyber incident is a cyber incident that is (or group of related cyber incidents) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.[19]

Analyzing the impacts of a significant cyber incident requires detailed knowledge of hundreds of dynamic variables that include the capabilities of the adversary, the behavior of the grid operators, and the real-time conditions of the electricity system.[v] As a result, a comprehensive understanding of how a cyberattack may impact the grid and its customers remains a significant gap for the intelligence community, industry, and subject matter experts. However, the U.S. electricity subsector stakeholders, in both government and private industry, perform regular assessments, exercises, and information sharing and coordination plans of general and specific responses to significant cyber incidents.

The U.S. Department of Energy (DOE) national laboratories, for example, develop and maintain significant capabilities to analyze cyber threats, electricity networks, ICS, and physical and cyber defenses; they regularly engage with the electric industry owners and operators to augment and support industry cybersecurity mechanisms (See Section 3.3.1). One recent unpublished study from the DOE national laboratories analyzed four cyberattack scenarios to assess a range of risks.[20] The simulated adversaries in these scenarios were highly sophisticated and capable of learning and adapting to cause the largest possible effect on the grid based on various amounts of electricity subsector knowledge and resources devoted to the attack. Each scenario attacked various known electricity subsector vulnerabilities, ranging from issues in the supply chains, issues related to the loss of similar components across multiple utilities, and issues related to

[v] This analytical gap to produce more unanimous products to assess cyber incidents is highlighted in the final section of this assessment.

widespread attacks on various critical electricity nodes across the country. In some instances, the simulated attackers could create the desired effects without damaging any infrastructure, only by issuing valid commands using ICS protocols.

Each scenario was modeled to simulate the impacts to the grid, measured in the amount of load (electricity consumption) disrupted or lost as a result of the simulated attack. The results of the study describe a range of load loss from 40 to 50,000 megawatts (MW), across the various scenarios.[vi] To create impacts in the higher range of estimates, the simulated attackers leveraged more sophisticated capabilities and significantly more time and resources; they also required highly detailed knowledge of the electricity subsector. While this range is not deliberately representative of current adversary capabilities or the current risks associated with a significant cyber incident, it does describe a possible scope of a significant cyber incident based on rigorous modeling and analysis from multiple DOE national laboratory experts.

To contextualize these modeled disruptions and inform the incident response capabilities and requirements of industry and governments, scope and duration is assessed through a review of (1) the electricity subsector's historical performance during power outages; (2) the unique electricity restoration characteristics that may change historical performance as a result of a significant cyber incident; and (3) the potential cascading impacts to national security, the economy, and public health and safety.

2.2 Historical Electric Grid Impacts from All Hazards

Understanding the scope and duration of a power outage due to a cyberattack requires an understanding of the likely performance of the electricity subsector during previous disruptions. The subsector has significant experience in responding to power outages of various scope and duration. Severe weather is the leading cause of power outages in the United States. Between 2003 and 2012, an estimated 679 widespread power losses occurred due to severe weather.[21] For decades, hurricanes and other severe weather events have impacted utilities in the eastern and southern United States. Massive ice storms, wild fires, and other natural hazards have also caused wide-area power outages in other U.S. regions.

The restoration of the grid is generally the same across all hazards. Electric utilities identify damage, isolate compromised systems, repair equipment, and restore power.[22] Electric utilities rely on detailed power restoration[vii] and business continuity plans, as well as pre-identified power restoration corridors to coordinate the logistical, workforce, and equipment resources needed to rapidly restore service following disruptions.[23]

[vi] For reference, the State of Illinois maintains roughly 45,500 MW of generation capacity. https://www.eia.gov/state/print.php?sid=il.

[vii] "The general technical process for grid restoration includes: Step 1: Power plants, are assessed for damage and restored; Step 2: High-voltage transmission lines are repaired; Step 3: Electric substations are brought online; Step 4: Power is restored to emergency services and facilities critical to public health and safety; Step 5: Crews are dispatched to repair lines that will return service to the largest number of customers in the least amount of time. Service lines to neighborhoods, industries, and businesses are systematically restored; Step 6: Once major repairs are completed, service lines to individual homes and smaller groups of customers are restored." (See endnote 23)

Today, most outages are local, brief, and caused by problems at the distribution level—such as lighting strikes, wind storms and tree falls, short circuits caused by squirrels, and other similar events. Based on Electric Disturbance Events data, of the events for which duration and either a load or customer count loss were reported from January 2002–April 2017, roughly 20% affected no customers, 75% affected between 1 and 500,000 customers, 4% affected between 500,000 and 1 million customers, and 2% affected more than 1 million customers (see **Figure 4**).[24]

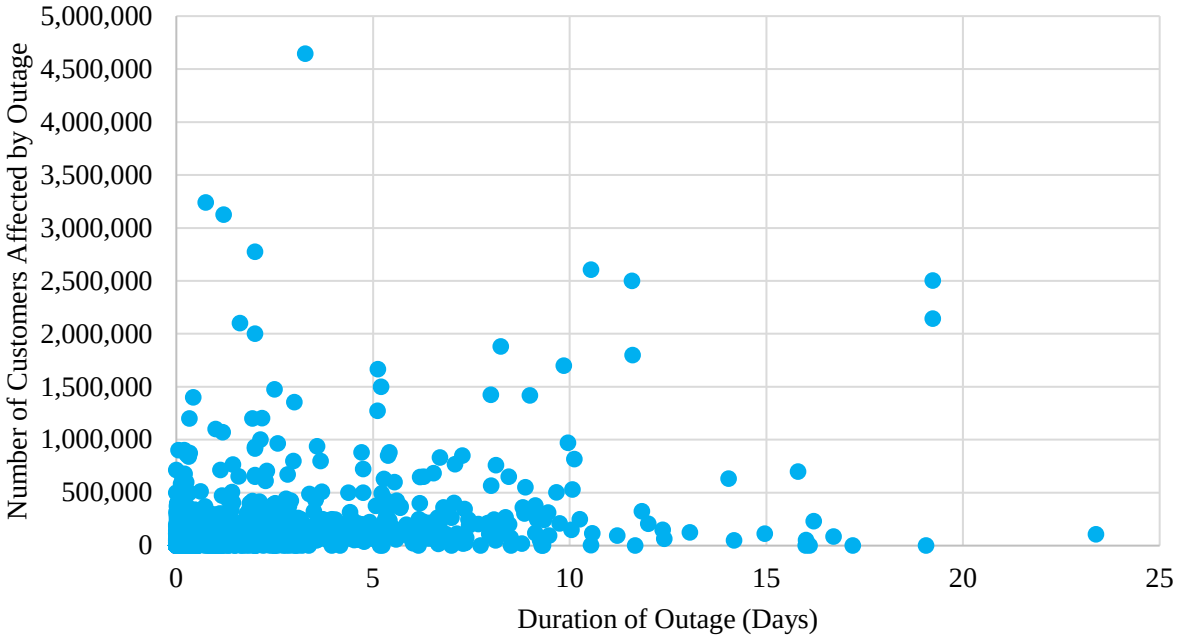

Figure 4. Reported Disturbances to the Electric Grid, Jan. 2002–Apr. 2017[viii]

While the restoration strategies are historically consistent across all hazards (see **Figure 5**), there is no "normal" restoration, especially considering large-scale incidents, which continue to create complex resource, logistics, and personnel challenges that often overwhelm the capacity of any single response entity. Many factors—including seasonally influenced demand, topography, population density, damage levels, inclement weather, and impacts to other critical infrastructure sectors that the electricity subsector relies on—can affect the rate of power restoration.

In some cases, electricity may be restored long before utilities fully recover from an incident. For example, the 2013 physical attack on the Metcalf substation resulted in no loss of electric service; however, it took the utility 27 days to fully restore the damaged equipment.[25] In instances with physical damages on a larger scale, such as an event that impacted a large number of large power transformers, it could take months, if not years, for equipment to be fully restored.[26] In partnership with the federal government, utilities are constantly taking steps to assess specific vulnerabilities and consequences to segments of their systems in an effort to drive investment in defensive capabilities, backup systems, or hardened infrastructure.

[viii] Duration is calculated as the length between the time an event began and the time of restoration, as reported by a utility in its OE-417 filing to report an electricity incident or disturbance to the Department of Energy.

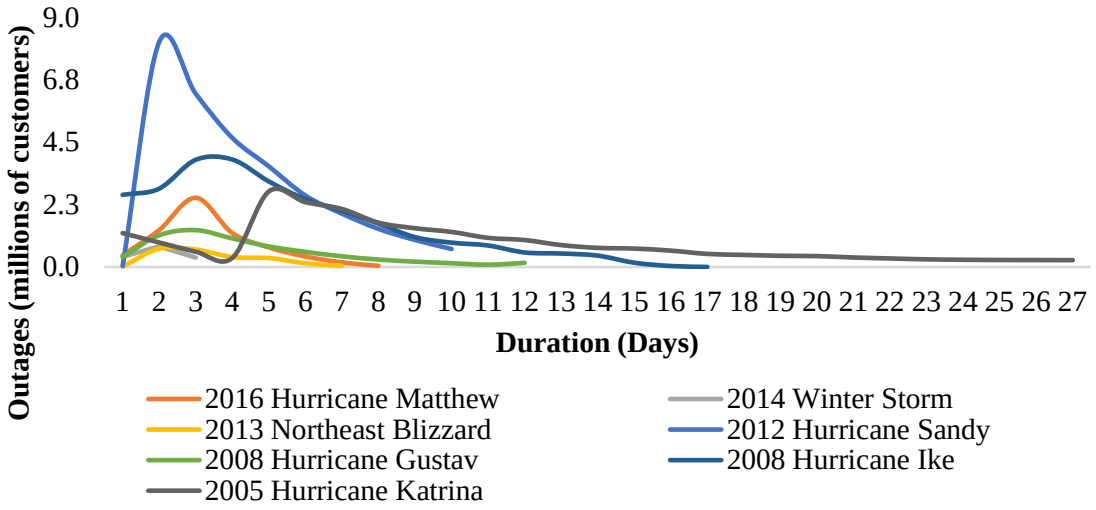

Figure 5. Number of Customers Impacted & Duration of Outage in Select Events[27]

2.3 A Significant Cyber Incident May Complicate Response and Restoration

Decades of experience in responding to natural- and manmade-disaster events has strengthened the United States' power restoration process. Assuming the restoration curve following a significant cyber incident is likely to be similar to those with previous DOE responses, power outages will be highest in the immediate aftermath of the disruption and then restoration will improve over time. However, many factors may complicate response to a significant cyber incident and the ability of the subsector to restore the electricity system to normal operating conditions (see **Figure 6**). As a result, the power restoration curve may shift up and to the right, resulting in more customers at risk of longer outages.

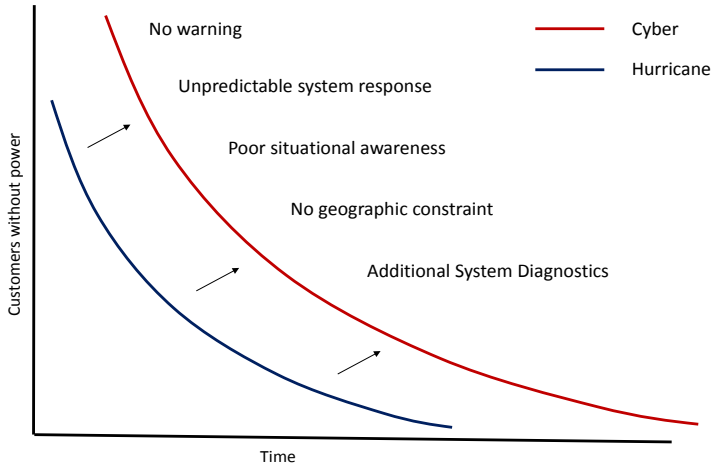

Figure 6. Power restoration curve may shift due to complications related to cyber incident

Cyber incidents may occur without warning. Estimates suggest that, with no preparation time, impacted entities would spend the first 12–24 hours of a no-notice cyber event standing up response teams and assessing system impacts.[28] These no-notice events introduce many variables not faced during a response to more predictable natural disasters, such as hurricanes. With no lead time, owners and operators are unable to take preemptive measures to protect their systems, develop restoration plans, or activate needed personnel. Interdependent sectors are also unable to take pre-incident steps to lessen the impact of losing electricity, including testing backup power systems and stockpiling supplies. The lack of advanced warning is cited as one of the factors contributing to a slower restoration time in the aftermath of the 2012 Derecho as compared to other weather events impacting the same region.[29]

Cyberattacks may selectively destroy specific types of components or facilities that are geographically dispersed throughout a network, or even the country. This may cause more unpredictable system responses than other outages that are more geographically contained. Grid operators may be exposed to new operating conditions if normally reliable support mechanisms—such as telecoms, IT systems, computer operating systems, which may be located far from the operator's normal impact areas—are rendered inoperable.

Existing mutual assistance programs, which provide tested, formal processes for impacted companies to request support from others during an outage, may be stressed in their response to a significant cyber incident due to the potentially widespread and unexpected nature. Also, as cyber incidents may impact disparate systems across the country, the impacted owner-operators may not be familiar with each other's systems and procedures.

Personnel resources required to recover from a cyber incidents may be different than what is required for more common hazards. Experts in ICS design, operation, and cybersecurity may be needed and not as readily available as others required during different outages. Other stakeholders of the electricity supply chain, including vendors of IT devices that support the grid, may need to be consulted if they are the victim of or impacted by a cyber incident. This may further delay the recovery.

The ability to ascertain system impacts during a cyber incident will likely be challenged by competing mandates and difficulties in sharing cyber information. Bulk power providers and government response personnel have indicated that it may take days, weeks, or potentially longer to identify the actual root causes of a significant cyber incident and to assess the associated grid impacts.[30] Additional system diagnostics, which are not required following most other hazard disruptions, may be necessary to ensure that restored systems are no longer vulnerable to strains of the attack, potentially extending restoration timelines.

While these complications could expand the scope and duration of the outages, grid owners and operators have efforts in place to prepare for, respond to, and recover from cyber incidents.[31] Preparedness and response capabilities are fostered through critical public-private partnerships focused on identifying risks, sharing information and intelligence, and enhancing response capabilities, among others (See Section 3.3.1 and Appendix A).[32]

2.4 Assessing the Impacts to the United States' National Security, Economy, and Public Health and Safety

The electricity subsector supplies energy services upon which all other sectors depend. To effectively assess the impacts of a power outage, it is critical to understand the complexities of the interactions between electricity and other critical infrastructures. While natural disasters can and have caused cascading failures, they are generally more contained in spatial extent, frequency, and duration; thus, the impacts of these types of events may be more predictable than those due to a cyber incident, which may be designed to target infrastructure interdependencies to create cascading failures across multiple sectors and systems.

Disturbances in other critical infrastructure sectors could cascade[ix] into the electricity subsector. Technical innovation and the development of digital information and telecommunications have increased both critical infrastructure efficiency and interdependency over the past half century.[33] Not only is the electric grid responsible for servicing more aspects of the modern economy than ever before, but the grid itself is now more dependent on other critical infrastructures. With trusted communications networks, remote access, mobile devices, vendors, and supply chains are the most likely routes of ingress.[34] Being able to accelerate power restoration to water systems, regional hospitals, communications nodes, and other critical facilities and functions will offer especially significant benefits. Helping utilities restore power before such problems jeopardize critical services can help prevent adversaries from achieving their objectives.

Beyond the electricity subsector, electric outages present impacts to national security, the economy, and public health and safety.[35] Infrastructure sectors recognize the criticality of their dependence on electricity and have invested resources in mitigating the effects of a power outage. However, prolonged outages present risk management challenges for other critical infrastructures and the important services they provide to the public and the economy.

The *2015 Energy Sector Specific Plan*, as required by the *National Infrastructure Protection Plan* (NIPP) (See Section 3.1.3 for more detail), details a number of specific interdependencies between the energy subsectors and other critical infrastructure sectors, including communications, transportation, financial services, and water.[36] Impacts to interdependent sectors may occur at the outset of an outage or, as may be the case where backup systems are deployed, within hours or days of initial power loss as backup systems fail, battery power is diminished, or fuel supplies for generators are depleted.

2.4.1 Assessing Impacts to National Security

The power grid is increasingly vital to U.S. national defense and homeland security. As defense and security capabilities evolve, so has their reliance on electricity to operate. The Center for Naval Analyses in a November 2015 report on the electric grid and national security noted that:

> *Assuring that we have reliable, accessible, sustainable, and affordable electric power is a national security imperative. Our increased reliance on electric power in every sector of*

[ix] Within the electricity subsector, a cascading event is one that starts as a small disturbance that is not contained by protective equipment and spreads in an uncontrolled manner. In this case, the term is used to refer to an event that starts in one system and spreads into another interconnected infrastructure.

> *our lives, including communications, commerce, transportation, health and emergency services, in addition to homeland and national defense, means that large-scale disruptions of electrical power will have immediate costs to our economy and can place our security at risk. Whether it is the ability of first responders to answer the call to emergencies here in the United States, or the readiness and capability of our military service members to operate effectively in the U.S. or deployed in theater, these missions are directly linked to assured domestic electric power.*[37]

Across the United States, the Department of Defense (DoD) relies on the electric grid to support military operations at home and abroad. As DoD pursues increasingly advanced capabilities, such as remotely piloted aircrafts and precision guided munitions, its ability to execute critical missions increasingly depends upon a vast and complex network of ground-based communications networks, radars, data centers, and command and control nodes that rely on electricity to operate. Approximately 85% of the energy infrastructure that DoD depends upon is commercially owned, and 99% of the electricity consumption of DoD installations is drawn from infrastructure outside these installations.[38] This dependence makes electricity reliability and resilience enormously important for national defense. While discussing reliance on commercial power supplies, DoD's *2015 Annual Energy Management Report* noted that, "DoD recognizes that such events could result in power outages affecting critical DoD missions involving power projection, defense of the homeland, or operations conducted at installations in the U.S. directly supporting warfighting missions overseas."[39]

Since 2008, DoD has taken aggressive actions through a broad range of initiatives to strengthen the ability of military bases and defense communications networks to operate on emergency backup power if blackouts occur, including providing backup generation at critical facilities. Even when operating on backup power, DoD has a deep interest in the expedited restoration of grid-supplied power, both to the base and to surrounding communities. Recognizing the growing importance of grid security and resilience to DoD mission assurance and national security, the federal government recently acquired new authorities—most prominently, the Grid Security Emergency Authority granted to the Secretary of Energy in the Fixing America's Surface Transportation Act (FAST Act) of 2015 (See Section 3.5)—to help reduce impacts and quicken restoration to critical grid components supporting defense missions.

Three of the five missions that DHS established in its *2014 Quadrennial Homeland Security Review* (QHSR) are related to the electricity system and the other critical infrastructure that depend on it: (1) preventing terrorism and enhancing security; (2) safeguarding and securing cyberspace; and (3) strengthening national preparedness and resilience.[40] The other two missions (securing our borders and enforcing our immigration laws) are supported by systems that rely on electricity. The Customs and Border Protection agency and Transportation Security Administration are two examples of agencies fulfilling DHS missions that rely on electricity to conduct their operations. The QHSR further highlighted the impact of aging and deterioration on critical infrastructure systems that ultimately weaken U.S. security and resilience to defend against increasingly sophisticated cyber incidents.

2.4.2 Assessing Impacts to the Economy

The costs of any power outage take various forms, including lost economic output and lost wages, spoiled inventory, delayed production, and damage to the grid and other infrastructure, among other factors. Between 2003 and 2012, power outages due to severe weather cost the economy an average of between $18 billion and $33 billion dollars each year, disrupting the lives of millions of Americans (see **Figure 7**).[41]

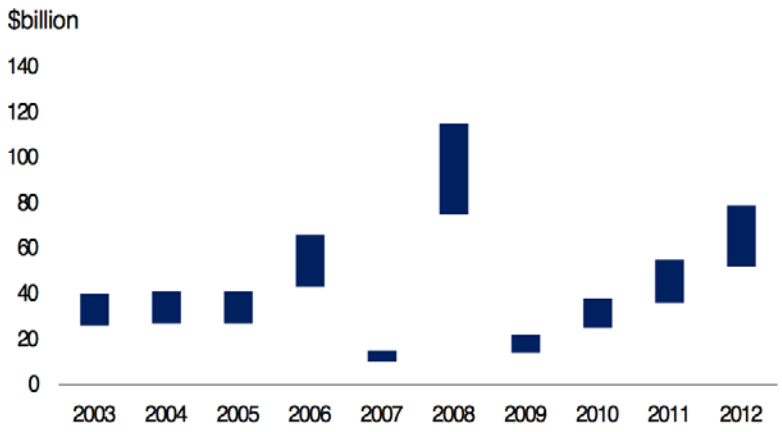

Figure 7. Range of Costs of Weather-Related Power Outages, Select Years

While the factors considered vary across each assessment of the economic costs of power outages, a brief description of the range of costs from key events illustrates the rough magnitude of economic impacts. For example, in 2008, the power outages associated with Hurricane Ike cost the economy between $24 billion and $45 billion, while power outages associated with Superstorm Sandy in 2012 led to impacts between $14 billion and $26 billion.[42] One of the largest power outages in recent history was not related to extreme weather. It began on August 14, 2003, when large portions of the Midwest and Northeast United States, as well as Ontario, Canada, experienced blackouts for up to 4 days and rolling blackouts for more than a week. Estimates of total costs in the United States from the event range between $4 billion and $10 billion.

There are several studies and models that have estimated the total cost of power outages in the United States, including those caused by weather- and non-weather-related events impacting various geographic areas.[43] Part of the challenge in assessing the impact of power outages on economic output is the considerable variation among sectors. Each sector (and subsector) will face its own challenges and employ its own resilience processes to reduce the economic impact of a power outage. Despite the difficulty of producing precise numbers, blackouts of large scale or long duration can easily result in economic costs of many billions of dollars.

2.4.3 Assessing Impacts to Public Health and Safety

The healthcare and public health sector recognized electricity is among the most vital of all infrastructure services because the loss of power could impact the delivery of healthcare services in inpatient healthcare facilities, outpatient care settings (e.g., dialysis facilities), and the homes of at-risk populations.[44, 45] Similar to other critical infrastructure sectors, the healthcare sector has

taken a number of steps to reduce its vulnerability to power disruptions, such as having backup generators onsite at healthcare facilities. During long-term power outages, healthcare facilities are likely to face limited fuel for backup generation and have difficulty sourcing new fuel supplies to supplement hospital stockpiles, which, according to one study, most often provide only enough fuel to run on generators for eight hours.[46]

The impact of power outages on health can be significant and far reaching. Power outages may strain the ability of healthcare facilities to deliver care as the demand for services increases. More than 2.5 million Americans rely on electricity-dependent medical equipment and medical devices.[47, 48] These individuals rapidly overwhelm emergency medical services, hospitals, and shelters as they seek access to secure power and care.[49]

A prolonged power outage may have impacts to public health beyond the provisions of healthcare services. Water monitoring and pumping, sewage treatment, food storage, and temperature control are all systems that rely on electricity and have a direct impact on public health if they are not powered. Without proper water treatment and delivery, and without refrigeration, access to clean water and fresh food may become limited. During power outages, people may also lose the ability to heat or cool their homes, which can be especially problematic if the outages occur during periods of extreme temperatures. In response to a prolonged power outage, the primary efforts of state emergency management agencies and the Federal Emergency Management Agency (FEMA) focus on addressing access to water, food, and housing.

During a power outage, it may be difficult for responders to communicate information to affected people. Electric means of communication would be interrupted by the power outage, so responders must find other methods of informing people of potential hazards associated with the outage (like contaminated water), as well as of ways to find fuel, food, water, and housing. In addition, the public may not be able to contact 9-1-1 emergency services if their phones run out of power. This will make sending and receiving information between the public and responders more difficult. This may also make informing law enforcement of increased criminal activity, like theft and looting, more difficult and contribute to public safety fears.

3.0 U.S. Readiness to Manage Consequences

The United States is, in general, well prepared to manage most electricity disruptions.[x] Federal agencies collaborate with stakeholders, such as the private sector and state, local, tribal, and territorial (SLTT) governments, under a broad set of national preparedness and response frameworks. Each stakeholder applies a diverse set of capabilities to address electricity supply disruptions. Appendix A provides a complete overview of federal capabilities for performing baseline cyber hygiene, defense, response, and recovery. Efforts to secure the electric grid against cyber vulnerabilities and long-term outages primarily occur within four lines of effort: (1) planning, (2) information sharing, (3) incident response, and (4) exercises to secure the electric grid against cyber vulnerabilities and prolonged outages. The government support to industry preparedness, response, and power restoration primarily occurs within three coordination structures: *the National Preparedness System,*[50] *the National Cybersecurity Incident Response Plan,*[51] *and National Infrastructure Protection Plan.*[52]

While the United States is generally well prepared, the network of incident management capabilities described in this section also highlights key gaps, which are addressed in Section 4 of this assessment. Gaps in capabilities and capacity exist around enhancing cyber incident response capacity, developing high-priority plans, augmenting scarce and critical resources, as well as understanding and characterizing response efforts to catastrophic incidents.

3.1 Planning

3.1.1 *National Preparedness System*

The *National Preparedness System* is designed to meet the *National Preparedness Goal* to build "a secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."[53] Components of the *National Preparedness System* include identifying and assessing risk, estimating the level of capabilities needed to address those risks, building or sustaining the required levels of capability, developing and implementing plans to deliver those capabilities, validating and monitoring progress, and reviewing and updating efforts to promote continuous improvement.

The *National Preparedness System* includes *National Planning Frameworks, Federal Interagency Operational Plans* (FIOPs), guidance for SLTT governments, and a full range of tools and processes for coordinating national preparedness efforts. Within the *National Preparedness System*, the cybersecurity core capability resides in the protection mission.[xi] Delivering this capability occurs across all mission areas, particularly in support of mitigation, response, and recovery activities. The federal government and many state governments organize

[x] The rationale for this conclusion stems from the widespread recognition of the criticality of electricity infrastructure and the state and scope of efforts across the United States—including industry and government efforts—to prepare for and manage the consequences of disruptions. As elaborated in this and the following section of this report, there are certain areas where catastrophic considerations and emerging threats reveal gaps in capabilities

[xi] The cybersecurity core capability is defined as "Protect (and, if needed, restore) electronic communications systems, information, and services from damage, unauthorized use, and exploitation."

response resources and capabilities under the National Response Framework's (NRF's) Emergency Support Function (ESF) construct. [xii]

For restoration and coordination of electricity subsector incidents, DOE leads many efforts through its role as the coordinating agency for ESF #12 – Energy under the NRF and as the sector-specific agency (SSA) for the energy sector pursuant to PPD-21. Based on these responsibilities, DOE's Infrastructure Security and Energy Restoration (ISER) team works closely with public and private sector stakeholders who secure the U.S. energy infrastructure against all hazards, reduce the impact of disruptive events, and respond to and facilitate recovery from major energy disruptions.

When activated for a disaster response operation, DOE has two main responsibilities:

- Provide Situational Awareness During Energy-Related Emergencies: Under the NRF, DOE is the lead for ESF #12. A key part of this role is collecting, evaluating, and sharing information on disaster impacts to energy infrastructure, as well as efforts to restore that damaged infrastructure. This situational awareness role may seem minor, but it is a critical component of the response operation. The information DOE collects is used by its partners in federal, state, and local governments to make decisions about the allocation of resources and to help develop public messaging.

- Facilitate the Restoration of Damaged Energy Infrastructure: In addition to its situational awareness role, DOE is also tasked with facilitating the restoration of damaged energy infrastructure. In most instances, this involves working with industry and federal agencies to process and approve transportation or environmental waivers. These waivers can help expedite response and recovery efforts following a disaster. The Power Marketing Administrations can also provide mutual assistance services to industry in extraordinary circumstances.

Some of the notable advances in national preparedness that augment the United States' ability to respond to a power outage resulting from a significant cyber incident include the following:

- Refreshed and updated *National Planning Frameworks*, including the first edition of the Protection mission area FIOP, home to the cybersecurity core capability.[54]

- *The Power Outage Incident Annex: Managing the Cascading Impacts from a Long-Term Power Outage (POIA*), detailing federal coordination processes and approaches for managing a long-term power outage event. The POIA guides and describes national emergency response efforts that occur simultaneously with energy restoration response efforts.

[xii] The NRF is a guide to how the United States responds to all types of disasters and emergencies. The framework describes the principles, roles, responsibilities, and coordinating structures for delivering the core capabilities required to respond to an incident; it further describes how response efforts integrate with those of the other mission areas.

- Increasingly mature national preparedness reports, detailing priority areas for capability development, which included a focus on augmenting national cybersecurity capabilities in 2015.

- *SLTT Plans and Annexes*, including *State Energy Assurance and Emergency Response Plans* developed in most states that detail the concept of operations and resource requirements for power outage scenarios.[55]

- Regularly conducted grid preparedness exercises performed by the U.S. government, SLTT partners, and electric companies to plan for a variety of emergency situations that could impact their ability to provide electricity or operate without it.[56]

3.1.2 *National Cybersecurity Incident Response Plan*

The *National Cyber Incident Response Plan* (NCIRP) was developed according to the direction of PPD-41 and leverages doctrine from the *National Preparedness System* to articulate the roles and responsibilities, capabilities, and coordinating structures that support how the United States responds to and recovers from significant cyber incidents posing risks to critical infrastructure.[57]

The NCIRP draws on guiding principles from PPD-41 to govern the federal government's response to any cyber incident, whether involving government or private sector entities.[58] While steady-state activities and the development of a common operational picture are key components of the NCIRP, the plan focuses on building the mechanisms needed to respond to a significant cyber incident. For significant cyber incidents, PPD-41 established the lead federal agencies and described the architecture for coordinating the broader federal government response for specified lines of effort.

The NCIRP also serves as the primary strategic framework for stakeholders when developing agency, sector, and organization-specific operational plans for responding to a significant cyber incident. The NCIRP serves as the basis for national cyber operational playbooks and individual critical infrastructure sector operational coordination plans; individual entities also reference it when developing their own plans. A key element in this restoration effort will be the asset response actions led by DHS' National Cybersecurity and Communications Integration Center (NCCIC) in close coordination with DOE as the SSA for energy. Recognizing the shared responsibility for cybersecurity the NCIRP also describes the federal government's coordination with the affected entity's response efforts.

In its role as SSA for the energy sector, DOE has implemented *Energy Sector Enhanced Coordination Procedures* that detail sector-specific procedures and concepts of operation that support the strategic framework of the *NCIRP*.

3.1.3 National Infrastructure Protection Plan

The United States' well-being relies upon secure and resilient critical infrastructure—the assets, systems, and networks that underpin American society. The *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013) outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes. NIPP 2013 meets the

requirements of *Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience*, signed in February 2013 and aligns with *Presidential Policy Directive 8 (PPD-8): National Preparedness*, signed in March 2011. The integration of physical security and cybersecurity planning is consistent with *Executive Order 13636, Improving Critical Infrastructure Cybersecurity*.

As part of NIPP, the public and private sector partners in each of the 16 critical infrastructure sectors and the SLTT government community have developed a *Sector-Specific Plan* that focuses on the unique operating conditions and risk landscape within that sector. In addition, joint national priorities have been identified under the NIPP framework based upon an evaluation of emerging risks, known capability gaps, resource availability, and best practices. The joint national priorities are intended to focus partner efforts as they implement activities to accomplish the remaining NIPP calls to action, to develop and implement updated Sector Specific Plans, and to pursue related efforts in furtherance of the NIPP 2013 strategic goals. Together, these joint priorities represent the community-wide distillation of the varied priorities pursued by individual government and industry entities. Within the NIPP partnership structure, the Electricity Subsector Coordinating Council (ESCC) serves as the principal liaison between leadership in the federal government and leadership in the electricity subsector and relevant associations, with the mission of coordinating and aligning efforts to prepare for national-level incidents or threats to critical infrastructure on all segments of the electricity system.

3.2 Information Sharing

The United States faces complex jurisdictional challenges to electric subsector reliability and resilience that are largely untested by a significant cyber incident. Components within the electricity distribution and transmission system are owned and operated by public utilities such as federal, state, or municipal governments; consumer-owned cooperatives; or investor-owned utilities. The variation in infrastructure ownership and operation and the jurisdictional overlap add complexity to sharing actionable information in a timely manner. These complexities are compounded when information is classified or sensitive due to the limited options and access to facilitate sharing.

3.3 Cyber Incident Response

During a significant cyber incident, asset response support from the federal government will be provided through a variety of mechanisms, including onsite incident response support from NCCIC teams at the request of the impacted parties. In all cases, incident response activities will be conducted in accordance with applicable law and policy, including the FIOP for Response and POIA.

ICS-CERT works closely with private sector asset owners, vendors, and government agencies at all levels (federal, state, local, and tribal) to protect America's critical infrastructure (CI) from cyber incidents. With these entities, ICS-CERT works to coordinate the sharing of information, services, and tools to help CI asset owners prevent, mitigate, and recover from cyber incidents and attacks. In FY 2016, the ICS-CERT incident response team completed work on 290 incidents. The energy sector accounted for 59 reported incidents.[59] Spear phishing represented 26% of these incidents, making it the leading access vector for ICS-CERT's FY 2016 incidents.

Also in FY 2016, the team responded to the first known cyber incident to result in physical impacts to a power grid. In another instance, they responded to an incident where an asset owner found low-level malware with persistent malicious remote access in its water control system.

As outlined in the NCIRP through the NCCIC, DHS leads the national cyber asset response efforts. To support tactical incident response efforts the NCCIC's Hunt and Incident Response Team (HIRT) provides incident response, management, and coordination activities for cyber incidents occurring in all 16 critical infrastructure sectors (including energy), as well as government entities at the federal and SLTT levels. HIRT provides NCCIC's operational capability for incident response and provides a variety of services, including onsite deployment teams. DHS would also seek to engage with Information and Communications technology providers as part of the incident response effort in order to incorporate industry expertise and experience.[xiii]

The Department of Justice (DOJ), through the Federal Bureau of Investigation (FBI) and the National Cyber Investigative Joint Task Force, leads threat response activities of the federal government to significant cyber incidents. These activities may include efforts to disrupt and dismantle the actions of nation-states, criminals, and terrorists to attack and undermine the U.S. electric grid. Hostile actors target the United States' critical infrastructure, including the electric grid, for computer network attacks and exploitation. Their purposes range from seeking national advantage against the U.S. economy, to threatening national security and/or public safety, to exploiting sensitive networks for unlawful monetary gain. DOJ and the FBI utilize all available investigative and prosecutorial tools to proactively identify, deter, disrupt, and dismantle such threats to the electric grid, as well as all critical infrastructure.

Supplemental crisis management coordination capability may be sought from other departments and agencies and funded through the Economy Act to support the lead federal agencies (i.e., DHS and the FBI) in conducting interagency coordination, situational awareness, crisis action planning, and other capabilities.

3.3.1 Stakeholder Capabilities

Industry: The ultimate responsibility for system operation and electricity restoration rests with the electricity subsector owners and operators who collectively own much of the U.S. energy infrastructure. Supply chain security for the equipment and software in these networks touches sourcing, vendor management, supply chain continuity and quality, transportation, and verification. In the global marketplace, vulnerabilities can be hard to avoid as components of equipment are made overseas and the use of general purpose components in electronics is increasing. Vendors work across multiple regions, so it is imperative to work with them for both technical assistance and to share information effectively about known vulnerabilities.

Electric subsector owners and operators have the resources necessary to respond to minor power outages,[60] and are constantly developing new capabilities to ensure they are better able to protect the subsector's critical infrastructure and to respond and recover should an incident occur.

[xiii] The President's National Security Telecommunications Advisory Committee delivered a report to the President on November 19, 2014 entitled, "NSTAC Report to the President on Information and Communications Technology Mobilization."

Frameworks, such as Edison Electric Institute's National Response Event Playbook and Regional Mutual Assistance Groups, for investor owned utilities have been developed to facilitate the rapid deployment of needed resources during response.[61] Mutual aid networks have also been developed to facilitate restoration for cooperative and municipal utilities by the National Rural Electric Cooperative Association and American Public Power Association, respectively. These networks allow impacted utilities to supplement their own resources with additional trained personnel, including linemen, engineers, vegetation crews, and support personnel provided by electric utilities from across the United States. To overcome cyber workforce challenges faced by many utilities, industry built on its mutual assistance concept by taking steps to develop a cyber mutual assistance (CMA) network at the direction of the ESCC. The voluntary CMA program seeks to identify entities that can provide services, personnel, and/or equipment on a voluntary basis to help restore computer systems following a significant cyber incident.

Despite CMA's development, these additional resources will likely be lacking during a significant cyber incident. During Hurricane Sandy, tens of thousands of additional personnel from more than 80 U.S. utilities traveled to the impacted area to support recovery efforts of the utilities hit.[62] The nature of cyber incident response necessitates a different, less pervasive skill set that may make leveraging CMA difficult at the time of an emergency. Additionally, while physical disruptions tend to be localized to a specific region of the country, a cyber incident may not be confined to a geographic area, limiting the "reach back" resources relied upon for mutual aid from utilities far away from the impacted areas.

Maintaining an inventory of spare components and equipment-sharing practices helps utilities mitigate the risk of long-term outages as a result of damage to large power transformers. These all-hazards response mechanisms—including Spare Transformer Equipment Program (STEP), SpareConnect, Grid Assurance, and RESTORE (Regional Equipment Sharing for Transmission Outage)—may provide valuable assistance during a cyberattack.

State, Local, Tribal, and Territory Governments: Government at all levels play important roles in enhancing preparedness and facilitating electricity restoration during large-scale events. The responsibility for responding to natural and manmade incidents generally begins at the local level with individuals and public officials in the county, parish, city, or town affected by an incident. State governments supplement local efforts before, during, and after incidents by applying in-state resources first. States can coordinate response efforts to substantial power outages through DOE's Energy Emergency Assurance Coordinators' Agreement that coordinates the efforts of the National Association of State Energy Officials, National Association of Regulatory Utility Commissioners, National Governors Association, and the National Emergency Management Association to prepare for and respond to energy disruptions. Many states have prepared for these efforts through the development of *State Energy Assurance Plans*.

If a state anticipates that its resources may be exceeded, the governor may request assistance from other states or through a Major Disaster or Emergency Declaration under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act). Federal coordination of emergency management response capabilities in support of the state(s) will be facilitated by FEMA at the Regional Response Coordination Center and at the National Response Coordination Center, as needed. In addition, FEMA has several grant programs available to

SLTT partners, as well as non-profits that address homeland security preparedness that recipients may use to address cyber capabilities.

During a significant cyber incident, state emergency management officials may need access to classified material and could access state fusion center capabilities, which serve as focal points for threat-related information sharing among SLTT partners, to receive the information needed to help manage incident response.

Regulators: Regulatory oversight of the electricity subsector at the national level is accomplished through two primary entities, NERC and FERC, and includes mandatory standards such as requiring all applicable entities to have a cybersecurity incident response plan, as well as a recovery plan for critical cyber assets. Regulatory oversight through the constantly evolving NERC Critical Infrastructure Protection Reliability Standards, including cybersecurity specific standards, ensures that utilities are implementing best practices to protect their systems. These standards are constantly evolving to ensure that protection keeps pace with the evolving threat environment. The electric industry has also been proactive in voluntarily adopting the National Institute of Standards and Technology's (NIST's) Cybersecurity Framework, which consists of standards, guidelines, and practices for organizations of any size to implement cybersecurity practices.

Reliability Coordinators: One essential coordination role for providing governance over the complex and distributed ownership of electric grid assets is that of the reliability coordinator. In large portions of the United States and Canada, the reliability coordinator role is performed by ISOs or RTOs, as they provide an independent operating view that includes both short and long-time horizons. This includes system planning across competing electricity utilities to ensure that generation capacity is available consistently across the regions of each reliability coordinator, as well as sufficient transmission systems to safely share power as it is distributed out to server customer load. The United States and Canada have a history of cross-border collaboration.[xiv] Both nations are long-standing members of NERC, and recognize it as the ERO and implementing partner for reliability standards across national and international jurisdictions. Mexico recently signed an agreement with the United States to work with NERC in its role as ERO, and it is working toward full membership.

Reliability coordinators also provide real-time situational awareness to adjust to changes in the electricity system, including localized outages of generation and transmission assets, as well as to provide coordination of resources from multiple competing utilities for the overall good of the electrical transmission system.

Public-Private Partnerships: A collective effort to enhance U.S. readiness to manage the consequences of a significant cyber incident requires public-private partnerships. Industry and government regularly collaborate on the development of new policies, standards, and regulations. Collaboration through industry-led efforts such as ESCC and Information Sharing and Analysis Centers (ISACs)—sector-specific, non-profit, member-driven organizations formed by critical

[xiv] In December 2016 the United States and Canada released the *Joint United States-Canada Electric Grid Security and Resilience Strategy* which has led to coordinated efforts by both nations on mutual issues of concern impacting their shared grid, including each country implementing a national action plan that addresses cross-border security concerns, including cybersecurity. [xiv]

infrastructure owners and operators—plays a critical role in cyber preparedness and response. The Electricity ISAC (E-ISAC), a division of NERC, works in close collaboration with key partners, including DOE and the ESCC, to fulfill its role as the primary security communications channel for the electricity industry, working to enhance industry's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents.[63] Another industry-led effort that supports response coordination is the ESCC Playbook, which streamlines senior leadership coordination and unity of messaging across industry and government.

Changes in technology and operation of the grid have created challenges for understanding roles and responsibilities for actions related to aspects of mitigation, response, and restoration in a cyber event. States are responsible for supporting electricity industry response to distribution impacts until resources are overwhelmed and a request for federal help is issued. The federal government has jurisdiction for impacts to transmission. Because regulatory authority is divided between federal, state, and sometimes local jurisdictions, utilities operate under varying regulatory frameworks due to regional differences, which makes "one size fits all" solutions particularly ineffective.[64]

3.4 Training and Exercises

The national preparedness community—including SLTT governments, the federal government, and industry partners—regularly conduct exercises to practice energy restoration activities. Training is an important component of the exercise process. Cyber response training that includes the unique knowledge of electrical grid operation and ICS should be more prevalent to develop the workforce necessary to prepare for a significant cyber incident impacting the grid.

Exercises such as NERC's Grid Security Exercise (GridEx)—where utilities demonstrate how they would respond to and recover from simulated, coordinated cyber and physical incidents—support the development of cyber response capabilities. Additional power outage emergency response exercises are conducted across the United States by SLTT and federal partners. These exercises strengthen operational and crisis communication relationships and provide input for lessons learned.

3.5 Authorities that Enable Response and Recovery

The federal government has a host of authorities that it can draw on to directly assist in response and recovery operations related to the electric grid in extreme circumstances. These include all-hazards emergency response authorities, as well as threat-specific authorities. In response to a significant cyber incident, the federal government may draw on authorities, including, but not limited to, those listed below. Certain authorities may be exercised independently, while others require consultation with other agencies or a presidential finding.

The National Cybersecurity Protection Act of 2014[65] amended the Homeland Security Act to codify the role of NCCIC as a primary federal-civilian interface for sharing information regarding cybersecurity risks and incidents and to authorize the NCCIC to provide cybersecurity-related technical assistance, risk management support, and incident-response capabilities to federal and non-federal entities.

The Cybersecurity Act of 2015[66] requires DHS to deploy technical capabilities to detect and prevent cybersecurity risks in the network traffic of federal agencies, and it requires agencies to apply those capabilities. The Cybersecurity Act of 2015 also establishes the NCCIC as the federal government's central hub for sharing cyber threat indicators between the private sector and the federal government and requires DHS to establish the federal government's capability and process for sharing cyber threat indicators with both federal and non-federal entities. Private entities sharing through this DHS capability in accordance with the Cybersecurity Act's requirements receive liability protection, as well as several other protections.

Section 215A(b) of the Federal Power Act[67] authorizes DOE, when the President identifies a "grid security emergency," to issue "emergency orders" to protect or restore critical electric infrastructure. Such emergencies are limited to geomagnetic storms, electromagnetic pulses, physical attacks, and cyberattacks, which significantly impact the reliability of the bulk power system. Other than geomagnetic storms, the emergency orders under section 215A of the Federal Power Act do not apply to natural disasters. The statutory description of what constitutes an "emergency order" is broad:

- DOE may issue "such orders for emergency measures as are necessary in the judgment of the Secretary to protect or restore the reliability of critical electric infrastructure or of defense critical electric infrastructure during such emergency."

- Orders may be issued without notice, hearing, or report.

- Orders may apply to any owner, user, or operator of critical electric infrastructure within the United States or ERO (currently NERC) and its associated regional entities.

Section 202(c) of the Federal Power Act[68] gives DOE the authority to order the establishment of temporary connections of facilities (e.g., transmission lines) or operation of generation facilities in the event of emergency situations, such as a sudden increase in demand, or shortage of electric energy.

The Defense Production Act[69] authorizes priority delivery/performance from American manufacturers on contracts and orders necessary for national defense—which has come to include critical infrastructure protection and restoration—or to maximize domestic energy supplies. Priority ratings are extended to every order within the procurement supply chain to obtain items or services needed to fill a rated order.

The Stafford Act[70] addresses two types of disaster declarations—major disaster declarations and emergency declarations. Both authorize the President to provide supplemental federal assistance to SLTT and insular area governments. In addition, certain not-for-profit organizations that own or operate a facility providing essential governmental type services may be eligible for assistance under FEMA's public assistance program. The type and amount of assistance differs depending on whether the Stafford Act Declaration is a major disaster or an emergency.

- Major Disaster Declaration—Under the Stafford Act, the President can issue a major disaster declaration for any natural catastrophe or (regardless of cause) any fire, flood, or explosion, in any part of the United States that the President determines causes enough damage to warrant major disaster assistance to supplement the efforts and available resources of states,

local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering that has ensued. A major disaster declaration provides a wide range of federal assistance programs for individuals and public infrastructure, including funds for both emergency and permanent work. Not being a natural catastrophe, a cyber incident or any other outage not inducted by natural events, generally would not qualify for a major disaster declaration, but would likely qualify under the broader definition of an emergency declaration. A fire, flood, or explosion caused by a cyber incident may qualify for a major disaster declaration.

- Emergency Declaration—The President can issue an emergency declaration for any occasion or instance when determined that federal assistance is needed to supplement SLTT or insular area government efforts and capabilities to save lives, protect property, protect public health and safety, or to lessen or avert the threat of a catastrophe in the United States. A power outage may qualify as an emergency under the Stafford Act. Such an incident resulting in a long-term power outage may qualify for an emergency declaration.

3.6 Conclusions

The national frameworks and systems for coordinating public and private sector risk management efforts are robust and sustained systems of plans, partnerships, and preparedness activities. In the last two years, the federal government has taken significant steps to enhance existing planning structures by significantly updating the concept of federal coordination for cyber incidents; creating incident-specific annexes to the response and recovery national planning frameworks focused on long-term power outages; and publishing a *National Cyber Incident Response Plan*.

National exercises focused on energy assurance and emergency response are important both for maintaining readiness and ensuring coordination among the diverse stakeholders and partners who manage the ecosystem of national preparedness and infrastructure risk management.

Despite taking steps to ensure their resilience to power disruptions, critical infrastructure sectors supporting the national economy, defense, and important lifeline functions remain vulnerable to power disruptions. The ability of government and industry partners to close identified gaps in cybersecurity preparedness and response capabilities can help reduce potential scope and duration of a significant cyber incident on the electric grid for the electric subsector, as well as interdependent critical infrastructure sectors.

4.0 Gap in Assets and Capabilities

Cybersecurity is one of six core capabilities highlighted for nationwide improvement in the *2016 National Preparedness Report*, and it is one of only three that has been consistently cited as an area for improvement since 2012.[71] Managing the consequences of a power outage associated with a cyber incident draws on a wide range of capabilities developed by a whole community of stakeholders and experts. Analysis, exercises, and industry assessments and initiatives generate an equally wide-ranging set of gaps, priorities, and long-term risk management initiatives.

Even though there are increasing investments and improvements in cybersecurity planning, information sharing, training, and countermeasures, major breaches involving business data in both public and private sectors underscore how vulnerable systems are to cyber threats. Gaps in capabilities in the electricity subsector highlight the major implications for the United States' national security, economy, and public health and safety posed by a potential long-duration, cyber-induced power outage.

This section outlines areas for improvement and high-level recommendations synthesized by reviewing existing national-level cybersecurity preparedness reports and examining themes and gaps. The purpose of this section is to (1) provide an overview of known capability gaps that have been identified through existing and ongoing studies, systems of national capability assessments, as well as key national-level exercises and analysis; and (2) propose recommendations to address major gaps and accelerate the adoption of cybersecurity measures in the electricity subsector.

4.1 Cyber Situational Awareness and Incident Impact Analysis

Existing capabilities for assessing potential consequence and impacts from cyber related disruptions and sharing relevant situational awareness in a timely and coordinated manner across sectors are often unable to provide the detail needed to better inform government executives, regulators, and utilities of potential risks, particularly of long term events. As described in Section 2, the electric subsector is interdependent with many other aspects of critical infrastructure, and actor capabilities from one sector can be translated to other sectors. The electricity subsector's primary existing situational awareness capability, Cybersecurity Risk Information Sharing Program, also known as CRISP, covers many, but not all, electricity customers in the U.S. However, it is limited to business networks of participating firms and wide-scale cyber situational awareness across operational infrastructure remains a critical gap. Additionally, there are no capabilities for entities to correlate cyber incident data in real time across multiple sectors. An increased situational awareness and incident impact analysis capability should be developed to leverage existing cybersecurity authorities and existing capabilities from across DOE national laboratories to provide modeling, analysis, and near real-time cybersecurity awareness of critical U.S. infrastructure. This gap is fostered in part by the lack of a streamlined processes for developing capabilities. Suggestions for improving cybersecurity impact analysis and capability gaps in the electricity subsector include the following:

- DOE, as the SSA, should work with NERC, the Defense Advanced Research Projects Agency, and other relevant organizations to assess the ability to expand cyber situational

awareness in the electricity subsector by enhancing tools such as DOE's Environment for Analysis of Geo-Located Energy Information, also known as EAGLE-I.

- DHS should work with cross-sector partners to develop cyber situational awareness across interdependencies that will provide cross-sector visibility, in real time, into cybersecurity incidents that occur in critical U.S. infrastructure to protect against cascading impacts.

- DOE, in coordination with DHS, should develop a program to continuously assess situational awareness information using subject matter experts in both cybersecurity and electricity to add context such as potential scope and duration of a significant cyber incident and impacts to cross-sector critical infrastructure systems.

- DOE, in collaboration with relevant partners, should conduct impact analyses to clarify and inform potential electric system costs related to cybersecurity that utilities can use to better inform investment decisions to secure the grid.

- DOE, DHS, and the U.S. Army Corps of Engineers should assess the sufficiency of data on industry back-up power to improve planning and modeling.

4.2 Roles and Responsibilities under Cyber Response Frameworks

Further clarity on the roles and responsibilities in responding to a cyber incident under the *National Preparedness System* is a common critique outlined by whole community partners. These procedures for coordination, resource deployment, and public messaging remain largely untested under real world conditions, thus leading to a further lack of clarity in how they would be operationalized. Clarifying operational roles and responsibilities during cyber incident response is an important component of enhanced preparedness. Similarly, communication seams between organizations cause confusion and reduce the ability of the whole community to mitigate impacts, protect health and safety, and improve response and recovery from a cyberattack. Suggestions for increasing clarity on roles and responsibilities under cyber response frameworks include the following:

- DOE, and DHS, in collaboration with relevant partners, should build on successful frameworks for natural disaster exercises such as DOE's Clear Path series to regularly convene industry, federal, and SLTT stakeholders on an annual basis for energy sector and cross-sector cyber response exercises to test and validate procedures aligned to the NCIRP.

- The electric industry should continue to integrate federal and SLTT partners into utility-hosted cyber incident exercises where appropriate.

- Government and industry should build a process to further the development of interdependency conscious restoration plans among cross-sector entities, specifically Section 9 companies.

- DOE should develop a team of cybersecurity experts with the requisite combination of technical knowledge in electricity and cybersecurity to complement direct assistance from DHS and other federal departments.

- The federal government, in coordination with SLTT and industry, should work through existing mechanisms—such as the ESCC, ESF-15, and ready.gov—to enhance its ability to communicate potentially sensitive cyber impacts to stakeholders during incidents and to coordinate preparedness during non-emergency periods.

- The federal government should codify relationships with industry to expedite technical assistance during response and clearly establish expectations for federal resources.

4.3 Cybersecurity Integration into State Energy Assurance Planning

The *2016 National Preparedness Report* concludes that while states focus more attention on cybersecurity by expanding the responsibility of state chief information security officers and investing a larger portion of their federal preparedness grants into improving cybersecurity planning and equipment, cybersecurity capabilities remain at risk of decline.[72] *2015 State Preparedness Report*s indicate that cybersecurity was the fifth-highest-rated priority, but the lowest rated in proficiency among all 31 core capabilities.[73] One specific gap in state cybersecurity preparedness is found in state energy assurance plans, which often do not fully incorporate cybersecurity concerns, including planning for long-term disruption events. Suggestions to overcome state energy assurance cybersecurity gaps include the following:

- States should work with DOE, DHS and industry partners to ensure that energy assurance plans align with industry efforts, as well as federal and state response structures.

- States should identify their exposure to impacts from events beyond their borders through analysis of potential vulnerabilities to regional energy supply chain impacts.

- States should ensure that energy assurance plans include the integration of cyber information sharing mechanisms such as the Multi-State ISAC.

- DOE should continue to support state and local planning and provide regional analysis of risk-based state energy assurance plans to identify gaps or overlapping resources that could hinder response and recovery nationally.

4.4 Electricity Cybersecurity Workforce and Expertise

It is important that the electricity subsector has a robust cybersecurity workforce that includes experts who can prepare for, respond to, and recover from cyber threats. However, the electricity subsector continues to face challenges recruiting and maintaining cybersecurity experts with strong knowledge of cybersecurity practices and the requisite knowledge of ICS used to operate the electric grid. Existing cybersecurity subject matter experts and related resources have limited bandwidth to fully support the full scope of electric subsector needs. The availability of trained cyber experts will likely be insufficient to meet the needs of all impacted entities during a

significant cyber incident, leading to competition between the public and private sectors and creating a shortage of cybersecurity leadership and expertise.[74] For example, while some utilities may have forensics teams able to determine the root cause of a cyberattack, many individual utilities likely lack the resources, expertise, and information necessary to conduct the necessary causal analysis and to rapidly deploy mitigation options for large-scale cyberattacks. Suggestions for supporting the development of an electricity subsector cybersecurity workforce include the following:

- Along with industry experts, federal and state governments should work with industry to assess the appropriate amount of personnel resources needed to support significant cyber incidents.

- DOE should identify methods for increasing government's capacity to support the electricity subsector's Cyber Mutual Assistance Program.

- Federal agencies, including the Department of Education, the National Science Foundation, the Department of Labor, DOE, NIST, and others, should continue and coordinate their ongoing efforts to sponsor the development and deployment of cybersecurity educational curricula to science, technology, engineering, and mathematics schools, community colleges, universities, and institutions of higher education for every stage of career development.

- DHS should establish a standard cybersecurity incident response qualification program for incident response personnel applicable to all sectors.

4.5 Supply Chain and Trusted Partners

Additional efforts are needed to facilitate further integration of cybersecurity across the electricity supply chain. This includes human resource considerations to protect against insider threats, as well as efforts to include cyber consideration into up-front areas of electric grid development through system design processes and system architectures. Adding on cybersecurity solutions after the fact can be expensive and, at times, less effective than if cybersecurity was incorporated throughout the design of ICS. Suggestions for facilitating the incorporation of cybersecurity throughout the electricity supply chain and with trusted partners include the following:

- DOE, in coordination with DHS, should support electricity subsector research, development, and deployment of system architectures and components, which help minimize cyberattack surfaces, prioritize key elements of electricity generation and delivery to isolate from internal and public networks, and enable system recovery.

- DOE should develop a national laboratory testing program for examining grid components to assess cybersecurity supply chain posture and examine cyber malware impacts to components in a simulated environment.

- DOE, in coordination with DHS, should engage ICS vendors to enhance vulnerability awareness and improve response.

- The federal government should develop strategies to further improve the resilience and security of precision timing and other risks to the electricity system.

- The federal government should develop methods to increase support to enhanced background checks for critical private sector employees that enhance security from insider threats.

4.6 Public-Private Cybersecurity Information Sharing

The *2016 National Preparedness Report* demonstrates the importance of cybersecurity information sharing between the public and private sectors, particularly in increasingly targeted industries.[75] The ability of all whole community partners to ensure effective cybersecurity information sharing through the bidirectional flow of information and intelligence between industry and government has been highlighted by all stakeholders as a continued challenge for the electricity subsector. The ability to ascertain system impacts during a cyber incident will likely be challenged by competing mandates and difficulty in sharing cyber information. Once information is available, barriers to sharing between government entities covering different jurisdictions and between government and industry threaten to reduce the ability of responding organizations to efficiently deploy resources. Bidirectional flow of information between the public and private sectors is impeded by the slow adoption of automated capabilities, while sharing classified information from government to industry in real time during a disaster remains a challenge.[76] Industry and government, in partnership with ISACs, could benefit from further clarity in roles, responsibilities, functions and objectives, expanded data sources, as well as improved information sharing capabilities. Suggestions for overcoming public-private cybersecurity information sharing gaps include the following:

- DOE should work with DHS, industry partners, and other relevant organizations to better define information needs and reporting thresholds through an assessment of voluntary and mandatory reporting requirements, such as the Electric Emergency Incident and Disturbance Report (OE-417) and NERC Reliability Standard EOP-004-2, as they relate to cyber incidents.

- Government, academia, and industry should improve tools for sector sourced intelligence and automated information sharing by scaling-up integration of machine-to-machine communication and artificial intelligence.

- DOE should develop a program for active protection of sensitive information, such as a robust critical electric infrastructure information, with appropriate confirmations of protection at federal and state levels that enables industry to enhance sharing with government in an environment separated from regulatory compliance.

- DOE, in coordination with DHS, should assess platforms to share classified or sensitive cyber-related information between public and private entities, as well as the accessibility of those systems for secure communication in steady-state and response.

- The federal government should enable the sharing of sensitive information between Section 9 organizations across all sectors.

- The federal government should expedite the publication of unclassified actionable threat information ("tear lines") for dissemination to non-cleared personnel to enable response to known threats.

- The federal government should streamline processes and methods for private sector clearances that prioritize individuals vital to national security.

- The Critical Infrastructure Partner Advisory Council (CIPAC) should be leveraged to establish a cross-sector, executive level, public-private mechanism to increase focus on risk mitigation.

4.7 Resources for National Cybersecurity Preparedness

There are many resources and tools available to utilities to improve response efforts; however, these resources and their applicability are not always well coordinated or understood among various cross-sector partners. Expanding this access could be fostered through continued DHS and DOE outreach and providing additional technical assistance to state utility commissions, relevant state and local agencies, and public and municipal utilities. Existing support to and clarity of methods for utilities to fund cybersecurity investments (particularly, smaller utilities) often falls short of the full scope of capabilities needed to improve prevention efforts. Additional efforts are needed from the U.S. government, states, public utility commissions, FERC, and other relevant officials to overcome existing gaps and barriers, to reallocate resources effectively, and to identify resource needs to ensure that the electricity subsector can effectively finance cybersecurity and incident recovery. Suggestions for overcoming resources for national cybersecurity preparedness gaps include the following:

- The federal government should coordinate efforts across DOE, DHS, and FERC to provide relevant cybersecurity tools to support mitigation strategies.

- DOE should assess the need for cybersecurity metrics to evaluate the costs and benefits of cybersecurity investments in the context of cost recovery mechanisms for utilities.

- The federal government should evaluate existing programs, such as FEMA grants, or create new programs to financially incentivize proactive electricity subsector cybersecurity measures.

- DOE should work with the insurance industry to further develop electricity subsector products, such as economic insurance from long-term power outages.

Appendix A. Cybersecurity Capabilities Catalogue for the Energy Sector

Functional Area: Identify

Description

The National Institute of Standards and Technology (NIST) Cybersecurity Framework defines the "Identify" function as "the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities." The Department of Homeland Security (DHS) offers qualitative and technical assessments to help organizations understand their cybersecurity risks.

U.S. Government Programs

DHS Programs:

- DHS Cybersecurity Advisors are regionally based experts assigned to help organizations within their areas of responsibility access U.S. government programs and maintain an ongoing relationship with the U.S. government.
- DHS offers two checklist-based risk assessments to supplement an organization's existing activities:
  - The Cyber Resilience Review (CRR) evaluates an organization's operational resilience and cybersecurity practices across 10 domains, including risk management, incident management, and continuity. The CRR may be conducted as a self-assessment or as an onsite assessment facilitated by a DHS cybersecurity expert. For more information, visit https://www.us-cert.gov/ccubedvp/assessments.
  - The Cybersecurity Evaluation Tool is a desktop software program that guides asset owners and operators through a step-by-step process to evaluate their industrial control systems and information technology (IT) network security practices. For more information, visit https://ics-cert.us-cert.gov/Assessments.
- Organizations interested in a technical assessment that simulates a malicious adversary may request an assessment from the National Cybersecurity and Assessment and Technical Services Team (NCATS). NCATS provides a variety of assessments to identify vulnerabilities in an organization's enterprise, including phishing tests, wireless application assessments, and internal penetration testing. For more information, email ncats_info@hq.dhs.gov.
- DHS Protective Security Advisors can provide additional assistance in conducting resiliency assessments and ensuring that critical services remain viable under all types of risks, including cyber. To learn more, visit https://www.dhs.gov/sites/default/files/publications/PSA-Fact-Sheet-508.pdf or email PSCDOperations@hq.dhs.gov.
- DHS works with the Department of Energy (DOE) and other sector-specific agencies (SSAs) to sponsor appropriate energy sector personnel for security clearances through the Private Sector Clearance Program. For more information, contact your Section 9 Program Manager.

DOE Programs:

- The Cybersecurity Capability Maturity Model (C2M2) program helps organizations perform consistent evaluation of the maturity of their cybersecurity capabilities for both IT and operations technology. The identification of gaps helps organizations prioritize their cybersecurity investments. C2M2 includes tailored versions of the model for the electricity and oil & natural gas subsectors and a sector-neutral version for cross-sector use. To learn more, visit http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program.
- The electricity subsector's cybersecurity Risk Management Process (RMP) guideline was developed by DOE, in collaboration with NIST and the North American Electric Reliability Corporation (NERC), specifically for the electricity subsector. The RMP's goal is to enable organizations—regardless of size or organizational or governance structure—to apply effective and efficient risk management processes and tailor them to meet their organizational requirements. To learn more, visit http://energy.gov/oe/services/cybersecurity/cybersecurity-risk-management-process-rmp.
- The Cybersecurity Risk Information Sharing Program facilitates voluntary, timely, and bidirectional exchange of cybersecurity threat information between electric utilities, the Electricity Information Sharing and Analysis Center (E-ISAC), and federal partners. The program integrates cyber threat information from program participants, with classified threat information from the U.S. government. For more information, email operations@eisac.com.
- DOE and DHS, in collaboration with other agencies and the intelligence community, provide classified and unclassified cybersecurity threat briefings and facilitate the sharing of industry best practice guidance.
- DOE can also call upon technical experts and resources from the national laboratories to assist energy sector organizations in identifying and understanding cybersecurity risks to systems, assets, data, and capabilities.

Other U.S. Government Programs:

- Within the government, the intelligence community facilitates the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.
- The Federal Bureau of Investigation (FBI), through its mission to investigate violations of federal law and threats to national security, collects evidence and intelligence to identify and disrupt potential threats, as well as to share actionable cyber threat intelligence. The FBI maintains a nationwide presence through its 56 field offices and "CyWatch," a 24/7 cyber command center—within the National Cyber Investigative Joint Task Force (NCIJTF).
- The FBI and the U.S. Secret Service (USSS) provide guidance on available federal resources and capabilities; through appropriate channels, promptly disseminate intelligence and information learned during threat response and other investigative activity; and facilitate information sharing and operational coordination with other federal government entities.

Functional Area: Protect

Description:
The NIST Cybersecurity Framework defines the "Protect" function as "the appropriate safeguards to ensure delivery of critical infrastructure services." DHS shares information about cybersecurity vulnerabilities to help organizations implement necessary safeguards based on the latest information available from government, industry, and the research community.

U.S. Government Programs:
DHS Programs:

- DHS offers regular alerts, warnings, and bulletins on cybersecurity vulnerabilities, mitigations, and best practices through the National Cybersecurity and Communications Integration Center (NCCIC). These alerts, warnings, and bulletins concern risks to general IT systems, as well as specialized risks to industrial control systems. All organizations should ensure regular receipt of relevant NCCIC products by appropriate cybersecurity personnel. Visit https://www.us-cert.gov/mailing-lists-and-feeds or email nccic@hq.dhs.gov for more information.

DOE Programs:

- DOE's Cybersecurity Energy Delivery Systems Research & Development program works with industry to develop innovative solutions to design resilience in energy delivery systems. To learn more, visit http://energy.gov/oe/services/technology-development/energy-delivery-systems-cybersecurity.

Functional Area: Detect

Description:
The NIST Cybersecurity Framework defines the "Detect" function as "appropriate activities to identify the occurrence of a cybersecurity event." An essential enabler of effective detection is the capability to exchange cyber threat indicators with a wide range of partners in real time. An additional key capability is the ability to conduct forensic analysis and identify potential adversary activity.

U.S. Government Programs:
DHS Programs:

- The flagship cybersecurity information sharing program within DHS is the Cyber Information Sharing and Collaboration Program (CISCP). CISCP provides a trusted forum where vetted partners share threat and incident information with the government and other private sector partners. CISCP also permits participating companies to submit personnel for security clearances and gain access to the NCCIC watch floor for operational collaboration similar to the DHS Infrastructure Protection Private Sector Clearance Program. For more information, email ciscp_coordination@hq.dhs.gov.
- DHS serves as the U.S. government's central hub for automated cyber threat indicator sharing. By participating in the Automated Indicator Sharing initiative, organizations share and receive machine-readable cyber threat indicators to immediately detect and block cybersecurity threats. For more information, visit https://www.us-cert.gov/ais.

- NCCIC provides forensic analysis of artifacts such as possible malware, phishing emails, and network logs to determine the existence or extent of a cybersecurity threat or incident. For more information, email nccic@hq.dhs.gov.
- DHS provides classified cyber threat indicators to cleared Commercial Service Providers (CSPs), which then use the indicators to protect their customers' unclassified systems. This program, Enhanced Cybersecurity Services, provides an added layer of protection for companies that enter in a contract with an approved CSP. To learn more, visit https://www.dhs.gov/enhanced-cybersecurity-services.

DOE Programs:

- DOE can call upon technical experts and resources from the national laboratories to assist energy sector organizations in protection activities.

Other U.S. Government Programs:

- Federal law enforcement and the intelligence community detect threats and share information to aid organization in identifying malicious cyber activity.

Functional Area: Respond

Description:

The NIST Cybersecurity Framework defines the "Respond" function as "the appropriate activities to take action regarding a detected cybersecurity event." DHS provides assistance to help organizations develop the capability to effectively respond after a cybersecurity compromise, and it offers onsite or remote support to directly address the immediate consequences of a breach.

U.S. Government Programs:

DHS Programs:

- Through the NCCIC Hunt and Incident Response Team (HIRT), DHS provides incident response, management, and coordination activities for cyber incidents occurring in the 16 critical infrastructure sectors, as well as government entities at the federal, state, local, tribal, and territorial (SLTT) levels. HIRT works with its constituents to identify and contain adversary activity and to develop mitigation plans for the removal and remediation of root cause. HIRT provides technical expertise and capacity to its constituents in responding to incidents. Incident response efforts are focused on finding the root cause of an incident by searching for techniques, tactics, and procedures, along with behaviors and associated artifacts in the victim network. For more information, email nccic@hq.dhs.gov.
- Through the National Cybersecurity Exercises and Planning Program, DHS facilitates exercises for government and private sector participants and offers templates for organizations to implement their own exercise programs. For more information, email nccic@hq.dhs.gov.
- When companies fall victim to a cybersecurity compromise, the NCCIC's Incident Response Team may provide onsite or remote assistance to help the victim understand the extent of the compromise, remove the adversary from their system, restore to a more secure state, and share key indicators of compromise with the government. For more information, email nccic@hq.dhs.gov.

- If a state anticipates that its response resources may be exceeded and the governor requests assistance, DHS through FEMA may be able to provide assistance through a Major Disaster or Emergency Declaration under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act).
- Defense Production Act authorities, which are jointly implemented by DHS, DOE, and five other federal agencies, may be available to support acquisition of critical system replacements.

DOE Programs:

- In accordance with Fixing America's Surface Transportation Act (FAST Act) of 2015, DOE may provide technical assistance to support cyber incident response for energy delivery systems. In its role as the SSA, DOE coordinates energy sector crisis state activities with DHS, the Department of Justice (DOJ), the intelligence community, the national laboratories, and other interagency partners. DOE can also call upon technical experts and resources from the national laboratories to assist energy sector organizations in response activities. For more information, email cyberenergy@hq.doe.gov.

Other U.S. Government Programs:

- DOJ, through the FBI and the (NCIJTF), is the federal lead agency for threat response activities. To learn more visit https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force.
- The FBI and USSS conduct appropriate law enforcement and national security investigative activity; collect evidence and gathering intelligence; identify additional affected entities; link related incidents and provide attribution; identify threat pursuit and disruption opportunities; develop and execute courses of action to mitigate the immediate threat; and facilitate information sharing and operational coordination with asset response elements.

Functional Area: Recover

Description:

The NIST Cybersecurity Framework defines the "Recover" function as "the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event."

U.S. Government Programs:

DHS Programs:

- The NCCIC Incident Response Team provides recommendations to help victim organizations restore their critical services and functions. For more information, email nccic@hq.dhs.gov.
- If the incident creates physical impacts, Stafford Act authorities may be available to States to support recovery operations.

DOE Programs:

- In the same way as DOE supports the 'Respond' phase, per the FAST Act of 2015, DOE may provide technical assistance to support recovery from cyber incident impacting energy delivery systems. In its role as the SSA, DOE coordinates energy sector crisis state activities with DHS, DOJ, intelligence community, the national laboratories, and

other interagency partners. DOE can also call upon technical experts and resources from the national laboratories to assist energy sector organizations in recovery activities.

Appendix B. Key Resources

The following is a list of key resources that inform the summary and conclusions contained in this assessment. While there are a wide range of resources available on the topics contained in this assessment, the documents included as key references here are useful guides for understanding the scope of activity within this area of assessment and are useful for characterizing the state of national capability and maturity in each area.

Key Authorities and References

- Executive Office of the President, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience* (Washington, DC: Executive Office of the President, 2013).
- Executive Office of the President, *Executive Order 13636, Improving Critical Infrastructure Cybersecurity*, February 2013.
- Executive Office of the President, *Presidential Policy Directive 8: National Preparedness* (Washington, DC: Executive Office of the President, 2011).
- Executive Office of the President, *Presidential Policy Directive 41: United States Cyber Incident Coordination* (Washington, DC: Executive Office of the President, 2016).

National Preparedness System Resources

- Federal Emergency Management Agency, *National Preparedness Goal* (Washington, DC: Department of Homeland Security, 2015), https://www.fema.gov/media-library/assets/documents/25959.
- Federal Emergency Management Agency, *National Planning Frameworks* (Washington, DC: Department of Homeland Security, 2015), https://www.fema.gov/national-planning-frameworks.
- Federal Emergency Management Agency, *Federal Interagency Operational Plans* (Washington, DC: Department of Homeland Security, 2015), https://www.fema.gov/national-planning-frameworks.
- Federal Emergency Management Agency, *National Preparedness Report* (Washington, DC: Department of Homeland Security, 2015), https://www.fema.gov/national-preparedness-report.

National Cyber Incident Response Plan Resources

- U.S. Computer Emergency Readiness Team, *National Cyber Incident Response Plan* (Washington, DC: Department of Homeland Security, 2016), https://www.us-cert.gov/ncirp.

National Infrastructure Security and Resilience Resources

- Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, DC: Department of Homeland Security, 2013), https://www.dhs.gov/national-infrastructure-protection-plan.

- Department of Homeland Security, *2015 Sector-Specific Plans* (Washington, DC: Department of Homeland Security, 2015) https://www.dhs.gov/2015-sector-specific-plans.

Energy Sector Specific Resources

- Department of Energy, *Emergency Support Function #12 – Energy Annex (to the Federal Interagency Operational Plan for Response*), May 2013, https://energy.gov/oe/downloads/emergency-support-function-12-energy-annex.
- Office of Infrastructure Security & Energy Restoration, *State, Local, Tribal and Territory Energy Assurance: 2016 Year in Review* (Washington, DC: Department of Energy, 2017), https://energy.gov/sites/prod/files/2017/04/f34/SLTT%20Energy%20Assurance%202016%20Year%20in%20Review_4.10.17.pdf.
- Electricity Subsector Coordination Council, *Initiatives*, March 2017, http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.6.
- *Electricity Subsector Coordinating Council Playbook*, Version 8.
- Department of Energy, *Clear Path IV Energy-Focused Disaster Response Functional Exercise (Clear Path IV) Summary Report* (Washington, DC: Department of Energy, 2016), https://www.energy.gov/sites/prod/files/2016/08/f33/ClearPathIV_Exercise%20Summary%20Report_Public%20Release.pdf
- Stephen M. Folga, Michael R. McLamore, Leah E. Talaber, and Angeli M. Tompkins, *National Electricity Emergency Response Capabilities* (Washington, DC: Department of Energy, August 2016) https://energy.gov/epsa/downloads/national-electricity-emergency-response-capabilities.
- Jason E. Stamp, Randall A. Laviolette, Laurence R. Phillips, and Bryan T. Richardson, *Final Report: Impacts Analysis for Cyber Attack on Electric Power Systems (National SCADA Test Bed FY08)* (Albuquerque, New Mexico: Sandia National Laboratories, 2009), http://prod.sandia.gov/techlib/access-control.cgi/2009/091673.pdf.
- Office of Energy Policy and Systems Analysis, *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats* (Washington, DC: Department of Energy, June 2016), https://energy.gov/epsa/downloads/electric-grid-security-and-resilience-establishing-baseline-adversarial-threats.
- Mission Support Center, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, Mission Support Center Analysis Report* (Idaho Falls, Idaho: Idaho National Laboratory, August 2016), https://energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf.
- Lloyd's and The University of Cambridge Centre for Risk Studies, *Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid, Emerging Risk Report 2015, innovation series* (London, UK: The University of Cambridge, 2015). https://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/business-blackout.

- SANS Industrial Control Systems, Electricity Information Sharing and Analysis Center, *Analysis of the Cyber Attack on the Ukrainian Power Grid, Defense Use Case* (Washington, DC: SANS Industrial Control Systems, Electricity Information Sharing and Analysis Center, March 18, 2016), https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
- Electricity Information Sharing and Analysis Center, *Internet of Things DDoS White Paper* (Washington, DC: Electricity Information Sharing and Analysis Center, October 24, 2016), https://www.eisac.com/api/documents/5689/publicdownload.
- North American Electric Reliability Corporation, *Grid Security Exercise GridEx III Report* (Washington, DC: North American Electric Reliability Corporation, March 2016), http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf.
- National Governors Association, *Preparing States for Extreme Electrical Power Grid Outages* (Washington, DC: National Governors Association, 2016), https://www.nga.org/files/live/sites/NGA/files/pdf/2016/1611PrepPowerGridOutages.pdf.
- Federal Energy Regulatory Commission, "News Release: FERC, NERC Staff Report Identifies Beneficial Practices for Grid Restoration and Recovery" January 2016, http://www.ferc.gov/media/news-releases/2016/2016-1/01-29-16.asp.
- Federal Energy Regulatory Commission, North American Electric Reliability Corporation, *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans* (Washington, DC: Federal Energy Regulatory Commission, North American Electric Reliability Corporation, June 2017), https://www.ferc.gov/legal/staff-reports/2017/06-09-17-FERC-NERC-Report.pdf.

References in Support of Interdependent Sectors

- *PLOS Currents*, "Table 5: A typology of health impacts of power outages," 2014, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3879211/table/d35e864/

Additional Resources

- *Stress Test Scenario: Sybil Logic Bomb Cyber Catastrophe* (University of Cambridge, UK: University of Cambridge Centre for Risk Studies, 2014). http://cambridgeriskframework.com/downloads
- *Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy* (University of Cambridge, UK: University of Cambridge Centre for Risk Studies, 2016). http://cambridgeriskframework.com/getdocument/40
- *BlackEnergy – Malware for Cyber-Physical Attacks* (Singapore, Singapore: iTrust Centre for Research in Cyber Security, University of Singapore, May 2016), https://goo.gl/wALXYw.
- Robert Knake, *A Cyberattack on the U.S. Power Grid, Contingency Planning Memorandum No. 31* (Washington, DC: Council on Foreign Relations, April 2017). https://www.cfr.org/report/cyberattack-us-power-grid.

- Richard Campbell, *Cybersecurity Issues for the Bulk Power System* (Washington, DC: Congressional Research Service, 2015), https://fas.org/sgp/crs/misc/R43989.pdf.
- Daniel Hurley, Jr., James Payne, Mary Anderson, *Critical Infrastructure: Electric Power—Subcommittee: Risk Mitigation in the Electric Power Sector: Serious Attention Needed,* Armed Forces Communication and Electronics Association Cyber Committee, http://www.afcea.org/committees/cyber/documents/AFCEA_Critical_Infrastructure_Final.pdf.
- R. Liu, *Integrated Simulation to Analyze the Impact of Cyber-Attacks on the Power Grid*, IEEE Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (2015). https://tcipg.org/sites/default/files/papers/2015_q1_gsa3.pdf
- Paul Stockton, *Superstorm Sandy: Implications for Designing a Post-Cyber Attack Power Restoration System* (Laurel, Maryland: Johns Hopkins Applied Physics Laboratory, 2016), http://www.jhuapl.edu/ourwork/nsa/papers/PostCyberAttack.pdf.

Appendix C. Endnotes

Executive Summary

[1] National Infrastructure Advisory Council, *A Framework for Establishing Critical Infrastructure Resilience Goals Final Report and Recommendations by the Council* (Washington, DC: National Infrastructure Advisory Council, October 2010), https://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf.
[2] According to NERC's "State of Reliability Report 2017," cyber vulnerabilities remain a high-risk profile relative to grid reliability. http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/SOR_2017_MASTER_20170613.pdf.
[3] Department of Homeland Security, "CrashOverride Malware," June 12, 2017, https://www.us-cert.gov/ncas/alerts/TA17-163A.
[4] Techniques, tactics, and procedures describe methods used by cyber adversaries to achieve their objectives. http://www.cisco.com/c/dam/en_us/about/security/intelligence/JNS_TTPs.pdf.
[5] Department of Defense, *The Department of Defense Cyber Strategy* (Washington, DC: Department of Defense, April 2015), https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.
[6] Richard Campbell, *Cybersecurity Issues for the Bulk Power System* (Washington, DC: Congressional Research Service, June 2015), https://fas.org/sgp/crs/misc/R43989.pdf.
[7] Mission Support Center, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, Mission Support Center Analysis Report* (Idaho Falls, Idaho: Idaho National Laboratory, August 2016), 4.
[8] NERC, "Frequently Asked Questions," November 2012, http://www.nerc.com/AboutNERC/Doents/FAQs_DEC12.pdf.
[9] According to *Presidential Policy Directive 41*, a significant cyber incident is a cyber incident that is (or group of related cyber incidents) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.
[10] National Research Council of the National Academies, *At the Nexus of Cybersecurity and Public Policy Some Basic Concepts and Issues* (Washington, DC: National Research Council, 2012).
[11] Department of Homeland Security, *The National Preparedness System* (Washington, DC: Department of Homeland Security, 2011), https://www.fema.gov/media-library-data/20130726-1828-25045-9792/national_preparedness_system_2011.pdf.
[12] Developed in alignment with *the National Preparedness System.* https://www.fema.gov/national-preparedness-system.
[13] Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, DC: Department of Homeland Security, 2013), https://www.dhs.gov/national-infrastructure-protection-plan.

Electric Sector Operations, Reliability, and Cybersecurity

[1] According to NERC, The bulk power system means facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and electric energy from generation facilities needed to maintain transmission system reliability. http://www.nerc.com/AboutNERC/keyplayers/PublishingImages/NERC_Interconnections_Color_072512.jpg.
[2] NERC, "Frequently Asked Questions," November 2012, http://www.nerc.com/AboutNERC/Doents/FAQs_DEC12.pdf.
[3] Edison Electric Institute, "Electric Reliability," http://www.eei.org/issuesandpolicy/electricreliability/Pages/default.aspx
[4] Navigant Consulting, Inc., *Evolution of the Electric Industry Structure in the U.S. and Resulting Issues* (Washington, DC: Electric Markets Research Foundation, October 2013), http://www.emrf.net/uploads/3/4/4/6/34469793/evolution_of_the_electric_industry_for_emrf_10-8-13.pdf.

[5] Department of Energy and Natural Resources Canada, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations* (U.S.-Canada Power System Outage Task Force, September 2006), https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf
[6] North American Electric Reliability Corporation, *State of Reliability 2017* (Washington, DC: North American Electric Reliability Corporation, June 2017), http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/SOR_2017_MASTER_20170613.pdf.
[7] North American Electric Reliability Corporation, *State of Reliability 2017* (Washington, DC: North American Electric Reliability Corporation, June 2017), http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/SOR_2017_MASTER_20170613.pdf. https://energy.gov/sites/prod/files/2017/01/f34/QER%20Transforming%20the%20Nations%20Electricity%20System%20Full%20Report.pdf.
[8] The Institute of Electrical and Electronics Engineers, "IEEE Benchmark Year 2016 Results for 2015 Data," 2016, http://grouper.ieee.org/groups/td/dist/sd/doc/Benchmarking-Results-2015.pdf
[9] Power System Engineering, Inc., "SCADA," 2017, http://www.powersystem.org/scada.
[10] Idaho National Laboratory, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector* (Idaho Falls, Idaho: Idaho National Laboratory, August 2016), https://energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf
[11] North American Electric Reliability Corporation, *State of Reliability 2017* (Washington, DC: North American Electric Reliability Corporation, June 2017), http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/SOR_2017_MASTER_20170613.pdf
[12] SANS Industrial Control Systems, "ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One)," January 2016, https://ics.sans.org/blog/2016/01/08/ics-cross-industry-learning-cyber-attacks-on-a-an-electric-transmission-and-distribution-part-one.
[13] Department of Homeland Security, "ICS-CERT Monitor, September 2015–February 2015," https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf. and Mission Support Center, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, Mission Support Center Analysis Report* (Idaho Falls, Idaho: Idaho National Laboratory, August 2016), 3.
[14] National Cybersecurity and Communications Integration Center, Industrial Control Systems Cyber Emergency Response Team, "FY 2016 Incidents," https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_IR_Pie_Chart_FY2016_S508C.pdf.
[15] Department of Homeland Security, "CrashOverride Malware," June 12, 2017, https://www.us-cert.gov/ncas/alerts/TA17-163A
[16] Department of Defense, *The Department of Defense Cyber Strategy* (Washington, DC: Department of Defense, April 2015), https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Scope and Duration of Prolonged Power Outage from A Significant Cyber Incident

[17] According to *Presidential Policy Directive 41*, a significant cyber incident is a cyber incident that is (or group of related cyber incidents) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.
[18] Statement of Scott I. Aaronson, Executive Director Security and Business Continuity Edison Electric Institute and Secretariat Member Electricity Subsector Coordinating Council, before The U.S. House of Representatives' Committee on Energy and Commerce Subcommittee on Energy, "The Electricity Sector's Efforts to Respond to Cybersecurity Threats" February 1, 2017.
[19] Executive Office of the President, *Presidential Policy Directive 41: United States Cyber Incident Coordination* (Washington, DC: Executive Office of the President, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.
[20] DOE Infrastructure Security and Energy Restoration report titled: Electricity Subsector Risk Characterization Study

[21] Executive Office of the President, *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages* (Washington, DC: Executive Office of the President, August 2013), https://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.
[22] Edison Electric Institute, "Understanding the Electric Power Industry's Response and Restoration Process," Washington, DC, October 2016, http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA_101FINAL.pdf.
[23] Edison Electric Institute, "Understanding the Electric Power Industry's Response and Restoration Process," http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/stormrestorationprocess.pdf.
[24] Department of Energy, Office of Electricity Delivery and Energy Reliability, Electric Disturbance Events (OE-417) Annual Summaries, https://www.oe.netl.doe.gov/OE417_annual_summary.aspx
[25] Congressional Research Service, "Testimony - Blackout! Are we Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?" April 11, 2016, https://transportation.house.gov/uploadedfiles/2016-04-14-campbell.pdf.
[26] Department of Energy, *Strategic Transformer Reserve, Report to Congress* (Washington, DC: Department of Energy, March 2017), https://energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf.
[27] Figure 5 derived from Department of Energy Office of Electricity Delivery and Energy Reliability Infrastructure Security and Energy Restoration Division Emergency Situation Reports, https://www.oe.netl.doe.gov/emergency_sit_rpt.aspx
[28] New York Independent System Operator and Department of Energy, *New York State Cybersecurity Exercise After Action Report*, January 2015.
[29] Office of Electricity Delivery and Energy Reliability, *A Review of Power Outages and Restoration Following the June 2012 Derecho Infrastructure Security and Energy Restoration* (Washington, DC: Department of Energy, August 2012), https://energy.gov/sites/prod/files/Derecho%202012_%20Review_0.pdf.
[30] New York Independent System Operator and Department of Energy, *New York State Cybersecurity Exercise After Action Report* (New York: NYISO, 2015)
[31] Statement of Scott I. Aaronson, Executive Director, Security and Business Continuity, Edison Electric Institute and Secretariat Member Electricity Subsector Coordinating Council, before The U.S. House of Representatives' Committee on Energy and Commerce Subcommittee on Energy, "The Electricity Sector's Efforts to Respond to Cybersecurity Threats," February 1, 2017.
[32] Federal Energy Regulatory Commission, North American Electric Reliability Corporation, *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recover Plans* (Washington, DC: Federal Energy Regulatory Commission and North American Electric Reliability Corporation, January 2016), https://www.ferc.gov/legal/staff-reports/2016/01-29-16-FERC-NERC-Report.pdf.
[33] Department of Energy, Department of Homeland Security, *Energy Sector Specific Plan* (Washington, DC: Department of Energy and Department of Homeland Security, 2015).
[34] Mission Support Center, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, Mission Support Center Analysis Report* (Idaho Falls, Idaho: Idaho National Laboratory, August 2016), 35.
[35] National Research Council of the National Academies, *At the Nexus of Cybersecurity and Public Policy Some Basic Concepts and Issues* (Washington, DC: National Research Council, 2012).
[36] Department of Homeland Security, *Energy Sector-Specific Plan* (Washington, DC: Department of Homeland Security, 2015), https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf.
[37] CNA Military Advisory Board, *National Security and Assured U.S. Electrical Power* (Arlington, VA: CNA, 2015)
[38] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Report of the Defense Science Board Task Force on DoD Energy Strategy "More Fight – Less Fuel* (Washington, DC: Department of Defense, February 2008).
[39] Office of the Assistant Secretary of Defense for Energy, Installations, and Environment, *Department of Defense Annual Energy Management Report Fiscal Year 2015* (Washington, DC: Department of Defense, June 2016)
[40] Department of Homeland Security, *The 2014 Quadrennial Homeland Security Review* (Washington, DC: Department of Homeland Security, June 2014), https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf

[41] Executive Office of the President, *Economic Benefits Of Increasing Electric Grid Resilience To Weather Outages* (Washington, DC: Executive Office of the President, August 2013), https://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.
[42] Executive Office of the President, *Economic Benefits Of Increasing Electric Grid Resilience To Weather Outages* (Washington, DC: Executive Office of the President, August 2013), https://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.
[43] National Research Council of the National Academies, *At the Nexus of Cybersecurity and Public Policy Some Basic Concepts and Issues* (Washington, DC: National Research Council, 2012).
[44] Department of Health and Human Services, Department of Homeland Security, *Healthcare and Public Health Specific Plan* (Washington, DC: Department of Health and Human Services, Department of Homeland Security, May 2016), 11; and Lin CJ, Pierce LC, Roblin PM, Arquilla B, "Impact of Hurricane Sandy on hospital emergency and dialysis services: a retrospective survey," *Prehosp Disaster Med*. 4, (2014): 374-9, doi: 10.1017/S1049023X14000715, https://www.ncbi.nlm.nih.gov/pubmed/25068276.
[45] Lin CJ, Pierce LC, Roblin PM, Arquilla B, "Impact of Hurricane Sandy on hospital emergency and dialysis services: a retrospective survey," *Prehosp Disaster Med*. 4, (2014): 374-9, doi: 10.1017/S1049023X14000715, https://www.ncbi.nlm.nih.gov/pubmed/25068276.
[46] Chaamala Klinger, Owen Landeg, and Virginia Murray, "Power Outages, Extreme Events and Health: A Systematic Review of the Literature from 2011–2012," *PLoS Currents Disasters* 1, (2014): doi: 10.1371/currents.dis.04eb1dc5e73dd1377e05a10e9edde673.
[47] Karen DeSalvo, Nicole Lurie, Kristen Finne, Chris Worrall, Alina Bogdanov, et al., "Using Medicare data to identify individuals who are electricity dependent to improve disaster preparedness and response," *Am J Public Health 104(7)*, (2014): 1160-4, doi: 10.2105/AJPH.2014.302009, https://www.ncbi.nlm.nih.gov/pubmed/24832404.
[48] Department of Health and Human Services, "HHS emPOWER Map 2.0 Shaping Decisions to Protect Health in an Emergency," https://empowermap.hhs.gov/HHSemPOWERMap2.0Factsheet_Final04072017.pdf.
[49]Prezant DJ, Clair J, Belyaev S, Alleyne D, Banauch GI, et al., "Effects of the August 2003 blackout on the New York City healthcare delivery system: a lesson for disaster preparedness," *Crit Care Med* 33, (2005):S96-101, https://www.ncbi.nlm.nih.gov/pubmed/15640685.

U.S. Readiness to Manage Consequences

[50] Department of Homeland Security, *The National Preparedness System* (Washington, DC: Department of Homeland Security, 2011), https://www.fema.gov/media-library-data/20130726-1828-25045-9792/national_preparedness_system_2011.pdf.
[51] Developed in alignment with *the National Preparedness System.*
[52] Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, DC: Department of Homeland Security, 2013) https://www.dhs.gov/national-infrastructure-protection-plan.
[53] Department of Homeland Security, *The National Preparedness System* (Washington, DC: Department of Homeland Security, 2011) https://www.fema.gov/media-library-data/20130726-1828-25045-9792/national_preparedness_system_2011.pdf.
[54] Federal Emergency Management Agency, "Federal Interagency Operational Plans," December 2016, https://www.fema.gov/federal-interagency-operational-plans
[55] Department of Energy, *State, Local, Tribal and Territory Energy Assurance: 2016 Year in Review* (Washington, DC: Department of Energy, 2016).
[56] Edison Electric Institute, "Understanding the Electric Power Industry's Response and Restoration Process," http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/stormrestorationprocess.pdf.
[57] *National Cyber Incident Response Plan* (Washington, DC: Department of Homeland Security, 2016), https://www.us-cert.gov/ncirp.
[58] Executive Office of the President, *Presidential Policy Directive 41: United States Cyber Incident Coordination* (Washington, DC: Executive Office of the President, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.
[59] Department of Homeland Security, National Cybersecurity and Communications Integration Center, Industrial Control Systems Cyber Emergency Response Team, *ICS-CERT Year in Review* (Washington, DC: Department of Homeland Security, 2016), https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf

[60] Risk and Infrastructure Science Center Global Security Sciences Division, Argonne National Laboratory, *National Electricity Emergency Response Capabilities* (Washington, DC: Department of Energy, August 2016), https://energy.gov/epsa/downloads/national-electricity-emergency-response-capabilities.
[61] Edison Electric Institute, "Understanding the Electric Power Industry's Response and Restoration Process," Washington, DC, October 2016, http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA_101FINAL.pdf.
[62] DOE Office of Electricity Delivery and Energy Reliability, *Overview of Response to Hurricane Sandy-Nor'easter and Recommendations for Improvement* (Washington, DC: Department of Energy, February 2013).
[63] The Electricity Information Sharing and Analysis Center, "About," https://www.eisac.com/#about.
[64] National Infrastructure Advisory Council, *Cyber Scoping Study Working Group*, February 16, 2017, https://www.dhs.gov/sites/default/files/publications/niac-cyber-scoping-study-powerpoint-02-16-17-508v2.pdf.
[65] *National Cybersecurity Protection Act of 2014*, Public Law 113-282 (128 Stat. 3066).
[66] *Cybersecurity Act of 2015*, Public Law 114-113 (129 Stat. 2935-85).
[67] *Federal Power Act*, 16 U.S.C. § 824o-1(b). The FAST Act, Public Law 114-94 (129 Stat. 1312), enacted December 4, 2015, amended the Federal Power Act to include the Grid Security Emergency authority.
[68] *Federal Power Act*, 16 U.S.C. § 824a(c).
[69] *The Defense Production Act of 1950, as amended*, 50 U.S.C. § 4501 et seq.
[70] *Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended*, Public Law 93-288 (88 Stat. 143), 42 U.S.C. §§ 5121-5207.

Gap in Assets and Capabilities

[71] Federal Emergency Management Agency, *National Preparedness Report* (Washington, DC: Department of Homeland Security, 2015), https://www.fema.gov/national-preparedness-report.
[72] Federal Emergency Management Agency, *National Preparedness Report* (Washington, DC: Department of Homeland Security, 2015), https://www.fema.gov/national-preparedness-report.
[73] Federal Emergency Management Agency, *National Preparedness Report* (Washington, DC: Department of Homeland Security, 2015), https://www.fema.gov/national-preparedness-report.
[74] National Infrastructure Advisory Council, *Cyber Scoping Study Working Group*, February 16, 2017, https://www.dhs.gov/sites/default/files/publications/niac-cyber-scoping-study-powerpoint-02-16-17-508v2.pdf.
[75] Federal Emergency Management Agency, *National Preparedness Report* (Washington, DC: Department of Homeland Security, 2015), https://www.fema.gov/national-preparedness-report.
[76] Federal Energy Regulatory Commission, North American Electric Reliability Corporation, *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans* (Washington, DC: Federal Energy Regulatory Commission, North American Electric Reliability Corporation, January 2016), https://www.ferc.gov/legal/staff-reports/2016/01-29-16-FERC-NERC-Report.pdf.