

Front-Line Resilience Perspectives: The Electric Grid

Global Security Sciences Division

About Argonne National Laboratory

Argonne is a U.S. Department of Energy laboratory managed by UChicago Argonne, LLC under contract DE-AC02-06CH11357. The Laboratory's main facility is outside Chicago, at 9700 South Cass Avenue, Argonne, Illinois 60439. For information about Argonne and its pioneering science and technology programs, see www.anl.gov.

DOCUMENT AVAILABILITY

Online Access: U.S. Department of Energy (DOE) reports produced after 1991 and a growing number of pre-1991 documents are available free via DOE's SciTech Connect (<http://www.osti.gov/scitech/>).

Reports not in digital format may be purchased by the public from the National Technical Information Service (NTIS):

U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Road
Alexandria, VA 22312
www.ntis.gov
Phone: (800) 553-NTIS (6847) or (703) 605-6000
Fax: (703) 605-6900
Email: orders@ntis.gov

Reports not in digital format are available to DOE and DOE contractors from the Office of Scientific and Technical Information (OSTI):

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831-0062
www.osti.gov
Phone: (865) 576-8401
Fax: (865) 576-5728
Email: reports@osti.gov

Disclaimer

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor UChicago Argonne, LLC, nor any of their employees or officers, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of document authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof, Argonne National Laboratory, or UChicago Argonne, LLC.

Front-Line Resilience Perspectives: The Electric Grid

prepared by
M. Finster, J. Phillips, and K. Wallace
Global Security Sciences Division, Argonne National Laboratory

prepared for
U.S. Department of Energy, Office of Energy Policy and Systems Analysis

November 2016

Contents

Acronyms	ix
Acknowledgments.....	xi
Executive Summary	xiii
1 Introduction.....	1
2 Information and Data Sources.....	5
3 Key Electric Grid Threats, Hazards, and Vulnerabilities	7
4 Resilience Enhancement Options.....	23
4.1 Hardening	23
4.1.1 Wind, Ice, and Snow Protection.....	24
4.1.2 Flood Protection	25
4.1.3 Buried Power Lines	27
4.2 Security Measures	27
4.2.1 Physical Security	27
4.2.2 Cybersecurity.....	28
4.3 Maintenance and General Readiness.....	29
4.4 Modernization, Control Enhancements, and Smart-Grid Technology.....	31
4.5 Diversified and Integrated Grid	33
4.6 Redundant Capabilities, Backup Equipment, and Inventory Management.....	36
4.7 Mutual Aid Programs	38
4.8 Succession Planning, Knowledge Transfer, and Workforce Development	40
4.9 Business Continuity and Emergency Action Planning	42
4.9.1 Customer Communication	43
4.9.2 Information Sharing.....	44
4.9.3 Exercises	45
4.10 Models	45
5 Challenges and Gaps in Addressing Resilience.....	49
5.1 Predictability of Storms and System Responses to Climate Change	50
5.2 Cost Recovery and Stranded Investments	50
5.3 Communication and Workforce.....	52
5.4 Coordination and Collaboration.....	53
5.5 Governance Gaps	55
5.6 Future Threats and Hazards.....	56

Contents (Cont.)

6	Conclusions.....	59
7	Works Cited.....	61
	Appendix A – Additional Information on Data Sources.....	A-1
	A.1 Electric Utilities and Utility Contractors.....	A-1
	A.1.1 Central Hudson Gas & Electric Corporation	A-1
	A.1.2 Public Service Electric and Gas Company Long Island	A-1
	A.1.3 Con Edison of New York.....	A-2
	A.1.4 Meade Electric Co.	A-2
	A.2 Publicly Available Sources.....	A-2
	A.2.1 North American Electric Reliability Corporation and Federal Energy Regulatory Commission.....	A-2
	A.2.2 U.S. Department of Energy Office of Electricity Delivery and Energy Reliability.....	A-3
	A.2.3 Quadrennial Energy Review	A-3
	A.2.4 National Association of State Energy Officials	A-4
	A.2.5 National Association of Regulatory Utility Commissioners.....	A-4
	A.2.6 Electric Power Research Institute.....	A-5
	A.2.7 Edison Electric Institute.....	A-5
	Appendix B – Detailed Information on Electric Grid Threats and Vulnerabilities	B-1
	B.1 Natural Hazards and Climate Change	B-1
	B.1.1 Ice, Snow, and Extreme Cold Weather.....	B-2
	B.1.2 Thunderstorms, Tornadoes, and Hurricane-Force Winds.....	B-3
	B.1.3 Increasing Temperature and Extreme Hot Weather	B-4
	B.1.4 Storm Surges, Flooding, and Increased Precipitation.....	B-5
	B.1.5 Earthquakes	B-6
	B.2 Direct Intentional Attacks.....	B-7
	B.2.1 Physical Attacks	B-7
	B.2.2 Cyber Attacks.....	B-8
	B.3 Geomagnetic and Electromagnetic Pulses.....	B-9
	B.4 Aging Infrastructure	B-10
	B.5 Capacity Constraints	B-11
	B.6 Workforce Turnover and Loss of Institutional Knowledge.....	B-11
	B.7 Human Error	B-12
	B.8 Dependencies and Supply Chain Interruptions.....	B-12

Figures

1	General Schematic of the Electric Power Grid	2
2	Electric Power Generation: Key Primary and Secondary Threats, Hazards, and Vulnerabilities	10
3	Electric Power Transmission: Key Primary and Secondary Threats, Hazards, and Vulnerabilities	13
4	Electric Power Distribution: Key Primary and Secondary Threats, Hazards, and Vulnerabilities	17
5	Consumption of Electric Power: Key Primary and Secondary Threats, Hazards, and Vulnerabilities	20
6	(a) Current Electric Grid (b) Diversified and Integrated Electric Grid	34
B.1	December 2013 Ice Storm in Lower Michigan.....	B-2
B.2	Wildfire Damage to Electric Distribution System Wood Poles.....	B-4

Tables

E.1	Identified Threats and Hazards against and Vulnerabilities of Electric Infrastructure	xiv
E.2	Electric Utility Resilience Enhancement Options	xv
E.3	Electric Utility Resilience Enhancement Options and Threats, Hazards, and Vulnerabilities Potentially Addressed	xvi
1	Descriptions of Data Sources and Their Roles in the Resilience of the Electric Grid	5
2	Identified Threats and Hazards against and Vulnerabilities of Electric Infrastructure	7
3	Electric Power Generation: Further Information for Key Primary and Secondary Threats, Hazards, and Vulnerabilities.....	11
4	Electric Power Transmission: Further Information for Primary and Secondary Key Threats, Hazards, and Vulnerabilities.....	14
5	Electric Power Distribution: Further Information for Key Primary and Secondary Threats, Hazards, and Vulnerabilities.....	18
6	Consumption of Electric Power: Further Information for Key Primary and Secondary Threats, Hazards, and Vulnerabilities	21
7	Hardening: Threats, Hazards, and Vulnerabilities Potentially Addressed.....	24
8	Security Measures: Threats, Hazards, and Vulnerabilities Potentially Addressed	29
9	Maintenance and General Readiness: Threats, Hazards, and Vulnerabilities Potentially Addressed	30
10	Modernization, Control Enhancements, and Smart-grid Technology: Threats, Hazards, and Vulnerabilities Potentially Addressed	33

Tables (Cont.)

11	Diversified and Integrated Grid: Threats, Hazards, and Vulnerabilities Potentially Addressed.....	35
12	Redundancy, Backup Equipment, and Inventory Management: Threats, Hazards, and Vulnerabilities Potentially Addressed.....	38
13	Mutual Aid Programs: Threats, Hazards, and Vulnerabilities Potentially Addressed	39
14	Succession Training, Knowledge Transfer, and Workforce Development: Threats, Hazards, and Vulnerabilities Potentially Addressed	42
15	Potential Business Continuity and Emergency Action Planning: Threats, Hazards, and Vulnerabilities Potentially Addressed.....	43
16	Models: Threats, Hazards, and Vulnerabilities Potentially Addressed	47
17	Electric Utility Resilience Enhancement Options	49

Acronyms

ASCE	American Society of Civil Engineers
CIP	Critical Infrastructure Protection
CIPC	Critical Infrastructure Protection Committee
CRISP	Cyber Risk Information Sharing Program
DER	distributed energy resource
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
EAP	energy assurance plan
EI	Edison Electric Institute
EGCC	Energy Sector Government Coordinating Council
EIA	U.S. Energy Information Administration
EPRI	Electric Power Research Institute
EPSA	Energy Policy and Strategic Analysis
ESCC	Electricity Subsector Coordinating Council
ES-ISAC	Electric Sector Information Sharing and Analysis Center
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
HSPD	Homeland Security Presidential Directive
IPCC	Intergovernmental Panel on Climate Change
ISO	International Standards Organizations
MS-ISAC	Multi-State Information Sharing and Analysis Center
NARUC	National Association of Regulatory Utility Commissioners
NASEO	National Association of State Energy Officials
NCSL	National Conference of State Legislatures
NEMA	National Emergency Management Association
NERC	North American Electric Reliability Corporation
NIMS	National Incident Management System
OE	Office of Electricity Delivery and Energy Reliability
PSE&G	Public Service Electric and Gas Company
PUC	Public Utility Commission
PwC	PricewaterhouseCoopers
QER	Quadrennial Energy Review

ROI	return on investment
SGMM	Smart Grid Maturity Model
SHRM	Society for Human Resource Management
SLEAP	State and Local Energy Assurance Program
SPC	Security, Preparedness, and Continuity

Acknowledgments

This document was prepared for Greg Singleton and Dr. Karen Wayland at the Department of Energy's Office of Energy Policy and Systems Analysis (EPSA). Argonne National Laboratory (Argonne) would like to thank a number of participants that donated their time and effort toward informing the results of this report, as well as the support of Mr. Singleton and Dr. Wayland for their encouragement and support throughout the process. Special thanks go to our industry and utility participants: Meade Electric Company, Central Hudson Gas & Electric Corporation, Public Service Electric and Gas Long Island, Consolidated Edison of New York; electric utility and policy subject matter experts at Argonne, especially Mr. Jeff Makar, Mr. Mike McLamore, and Mr. Jeff Pillon; and Ms. Stephanie Hamilton at Brookhaven National Laboratory who facilitated discussions with utility representatives.

This page intentionally left blank

Executive Summary

The United States has one of the world's most reliable, affordable, and increasingly clean energy-based electric power systems. At the core of the electric system is the grid, a highly complex, engineered, and interconnected network that connects the production and delivery of power to customers. Electricity enables and supports all critical infrastructure sectors, and our society's dependence on electricity only continues to increase. Because of its importance as a national security and economic asset, in combination with its extensiveness and visibility, the electric grid can be viewed as quite vulnerable to numerous manmade threats and natural hazards. However, the design of the grid also has the potential to make it quite resilient, meaning it has the ability to minimize disruptions to energy service by anticipating, resisting, absorbing, responding to, adapting to, and recovering from a disturbance. States and utility companies are at the front lines of assuring this system resilience. This report seeks to summarize how states and local utility companies are approaching all-hazards resilience in planning, construction, operations, and maintenance of the electric system, as well as challenges faced when addressing all-hazards resilience. What follows is a series of findings and insights from stakeholders and experts involved with the day-to-day mission of ensuring electricity system resilience. As much of this work is based on discussions and observations, these insights are not conclusive, yet represent the views of the individuals and institutions charged with maintaining and operating the electricity system on a daily basis. As such, these insights are suggestive of developing areas and topics for further exploration. Supporting data were collected from open source research, national electric associations, and interviews with electric utilities.

In addition to the electric utility and industry input, publicly available documents, reports, and proceedings from the following national organizations supported the construction of this report:

- North American Electric Reliability Corporation
- Federal Energy Regulatory Commission
- U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability
- Quadrennial Energy Review
- National Association of State Energy Officials
- National Association of Regulatory Utility Commissioners
- Electric Power Research Institute
- Edison Electric Institute

In general, threats and hazards can be viewed as anything that can disrupt or impact a system. Many threats and hazards to critical electricity infrastructure are universal (e.g., physical attacks), while others vary by geographic location and time of year (e.g., natural disasters). Threats and hazards also range in frequency of occurrence, from highly likely to occur (e.g., weather-related events) to incidents less likely to occur (e.g., electromagnetic pulse). Vulnerabilities (i.e., aging infrastructure) are points of weakness that exist within a system that increase its risk and susceptibility to adverse effects. On the basis of discussions with the utilities, as well as research, common issues and problems were identified regardless of source. Table E.1 displays the different identified threats, hazards, and vulnerabilities grouped into three general categories: natural hazards; direct intentional threats; and other threats, hazards, and vulnerabilities. Overall, the most critical threats, hazards, and vulnerabilities to the electric

Table E.1 Identified Threats and Hazards against and Vulnerabilities of Electric Infrastructure

Natural Hazards		Direct Intentional Threats		Other Threats, Hazards, and Vulnerabilities	
	Ice, snow, and extreme cold weather		Physical attacks		Geomagnetic and electromagnetic pulses
	Thunderstorms, tornadoes, and hurricane-force winds		Cyber attacks		Aging infrastructure
	Storm surge, flooding, and increased precipitation		---		Capacity constraints
	Increasing temperature and extreme hot weather		---		Workforce turnover and loss of institutional knowledge
	Earthquakes		---		Human error
	---		---		Dependencies and supply chain interruptions

distribution system are related to increased extreme weather and climate change and the aging of the infrastructure itself. Resulting concerns include extreme storms and the related impact of falling branches and trees on infrastructure; the effect of increased precipitation, sea-level rise, and storm surge on flooding; and the greater power demand on the distribution system due to extreme heat and/or cold and system component failure (e.g., pole deterioration, overhead and underground cable deterioration and faults, overloaded switchgears, and transformers).

Discussions and research further revealed the numerous options utilities are actively pursuing with regard to increasing resilience against these threats and hazards. Table E.2 illustrates some common resilience enhancements, with examples, as identified by utilities and research. Table E.3 cross-references each identified resilience enhancement with the various threats, hazards, and vulnerabilities that options could potentially address.

In general, the primary goals for utilities are to protect the system, reduce the impact of damage sustained, reduce the area affected by damage, and improve restoration time. As a result, the utilities' focus has frequently centered on component hardening against natural hazards (e.g., wind, ice, snow, flooding, etc., as regionally applicable), enhanced vegetation management, infrastructure protection/replacement, technology and control enhancements, and modernization improvements. However, the most significant investment utilities are making toward resilience include the installment and implementation of advanced meters and smart-grid technology.

Table E.2 Electric Utility Resilience Enhancement Options

Resilience Enhancement Options	Definition	Example
Hardening	Physical changes that improve the durability and stability of specific pieces of infrastructure	Raising and sealing water-sensitive equipment
Security measures	Measures that detect and deter intrusions, attacks, and/or the effects of manmade disasters	In-depth security checks on all employees, badged entry and limited access areas, and surveillance and monitoring
Maintenance and general readiness	Routine efforts to minimize or prevent outages	Vegetation management and regular inspection and replacement of worn-out components
Modernization, control enhancements, and smart-grid technology	Technology and materials enhancements to create a more flexible and efficient grid	Integration of smart-grid technologies, such as smart meters and phasor measurement units
Diversified and integrated grid	Transitioning of the grid from a centralized system to a decentralized generation and distribution system	Integration of distributed generation sources, such as renewable energy sources and establishment of microgrids
Redundancy, backup equipment, and inventory management	Measures to prepare for potential disruptions to service	Maintenance of spare equipment inventory, priority agreements with suppliers, and maintenance of a supply of backup generators
Mutual aid programs	Agreements that encourage entities to plan ahead and put in place mechanisms to acquire emergency assistance during or after a disaster	Agreements between utilities to send aid or support after a disaster
Succession training, knowledge transfer, and workforce development	Planning for transfer of knowledge and skills from a large retiring workforce, to a smaller, younger workforce	Proactive efforts to create training and cross-training programs and succession plans
Business continuity and emergency action planning	A formal plan that addresses actions and procedures to maintain operations preceding an event	Components including employee awareness, training, and exercising
Models	Mathematical constructs that provide information on performance and/or disruptions to aide in decisionmaking	Probabilistic risk models to assist in predicting outage impacts after an event

Table E.3 Electric Utility Resilience Enhancement Options and Threats, Hazards, and Vulnerabilities Potentially Addressed

Resilience Enhancement Options	Threats, Hazards, and Vulnerabilities Addressed (primary in regular font; secondary in italics)	
Hardening	 Thunderstorms, tornadoes, and hurricane-force winds  Earthquakes  Geomagnetic and electromagnetic pulses  <i>Human error</i>	 Storm surges, flooding, and increased precipitation  Physical attacks  Cyber attacks
Security measures	 Physical attacks  Human error	 Cyber attacks
Maintenance and general readiness	 Thunderstorms, tornadoes, and hurricane-force winds  Earthquakes  Human error  Dependencies and supply chain interruptions  <i>Increasing temperature and extreme hot weather</i>	 Storm surges, flooding, and increased precipitation  Aging infrastructure  Workforce turnover and loss of institutional knowledge  <i>Ice, snow, and extreme cold weather</i>  <i>Capacity constraints</i>
Modernization, control enhancements, and smart-grid technology	 Ice, snow, and extreme cold weather  Cyber attacks  Human error	 Thunderstorms, tornadoes, and hurricane-force winds  Aging infrastructure  <i>Capacity constraints</i>
Diversified and integrated grid	 Ice, snow, and extreme cold weather  Storm surges, flooding, and increased precipitation  Earthquakes  Human error	 Thunderstorms, tornadoes, and hurricane-force winds  Increasing temperature and extreme hot weather  Capacity constraints  Dependencies and supply chain interruptions

Table E.3 (Cont.)

Resilience Enhancement Options	Threats, Hazards, and Vulnerabilities Addressed (primary in regular font; secondary in italics)	
Redundancy, backup equipment, and inventory management	 Ice, snow, and extreme cold weather  Storm surges, flooding, and increased precipitation  Earthquakes  Capacity constraints  Dependencies and supply chain interruptions	 Thunderstorms, tornadoes, and hurricane-force winds  Increasing temperature and extreme hot weather  Aging infrastructure  Human error  <i>Physical attacks</i>
Mutual aid programs	 Ice, snow, and extreme cold weather  Storm surges, flooding, and increased precipitation  Earthquakes  Aging infrastructure  Workforce turnover and loss of institutional knowledge	 Thunderstorms, tornadoes, and hurricane-force winds  Increasing temperature and extreme hot weather  Physical attacks  Capacity constraints  Dependencies and supply chain interruptions
Succession training, knowledge transfer, and workforce development	 Physical attacks  Geomagnetic and electromagnetic pulses  Workforce turnover and loss of institutional knowledge  Dependencies and supply chain interruptions  <i>Thunderstorms, tornadoes, and hurricane-force winds</i>  <i>Increasing temperature and extreme hot weather</i>  <i>Aging infrastructure</i>	 Cyber attacks  Capacity constraints  Human error  <i>Ice, snow, and extreme cold weather</i>  <i>Storm surges, flooding, and increased precipitation</i>  <i>Earthquakes</i>

Table E.3 (Cont.)

Resilience Enhancement Options	Threats, Hazards, and Vulnerabilities Addressed (primary in regular font; secondary in italics)	
Business continuity and emergency action planning	 Ice, snow, and extreme cold weather  Storm surges, flooding, and increased precipitation  Earthquakes  Cyber attacks  Human error	 Thunderstorms, tornadoes, and hurricane-force winds  Increasing temperature and extreme hot weather  Physical attacks  Geomagnetic and electromagnetic pulses  Dependencies and supply chain interruptions
Models	 Ice, snow, and extreme cold weather  Storm surges, flooding, and increased precipitation  Earthquakes  Cyber attacks  Aging infrastructure  Dependencies and supply chain interruptions	 Thunderstorms, tornadoes, and hurricane-force winds  Increasing temperature and extreme hot weather  Physical attacks  Geomagnetic and electromagnetic pulses  Capacity constraints

Advanced smart-grid systems can be used to expedite information flow; remotely monitor demand, performance, and quality of service; enhance system efficiency; and improve outage detection and restoration by identifying the location and description of damaged equipment. Real-time monitoring data can also support hourly pricing and reactive power and/or demand response programs, which allow utilities to make same-day operational decisions, near-term forecasts, and scenario evaluations. Historical data, coupled with predictive modeling of extreme weather events and the related effects on electric infrastructure, are also used to inform management decisions, identify areas of greatest risk, ascertain system vulnerabilities, allocate resources, and help prioritize investments.

Utilities also typically have backup inventory on hand to supply an expanded workforce with all necessary restoration material for 2–3 days, although a restoration effort that extends beyond this, with a significantly expanded workforce, could require some level of restocking before the restoration work is complete. Furthermore, most electric utilities have assistance arrangements and sharing mechanisms in place to facilitate aid and emergency assistance during or after a disaster. In addition, when responding to outage events, two-way communication with customers and other stakeholders is nearly as important as the actual restoration of service. Websites are now frequently used as the interface to relay and receive important incident-related information,

such as outage maps, status of outages, preparation checklists, special needs requests, and safety concerns/issues.

Despite all the work underway to ensure the grid can withstand, recover, and restore operations quickly, barriers and gaps still remain that make additional resilience enhancements challenging to implement. Addressing and working to remedy these barriers and gaps are needed to continue to make progress toward a more resilient grid. The list below explains these barriers (see Section 5 for additional detail):

1. **Cost Prohibitive:** Resilience enhancement options can be very expensive and may not provide noticeable immediate return on investment. Thus, when considering new initiatives, routine maintenance, and system upgrades, utilities must constantly balance the demand for and impact of reduced risk, improved reliability, and enhanced resilience on the most critical assets, with the overall cost, uncertainty rounding cost recovery, and associated funding burden to rate payers (i.e., reasonable and prudent recovery of cost).
2. **Policy Barriers:** Many gaps and ambiguities inhibit resilience enhancement measures, including development of state and local policies and regulations regarding energy infrastructure resilience that can potentially be prohibitive (although sometimes beneficial) to resilience in the long run.
3. **Uncertainty Regarding Dependencies and Interdependencies:** The incomplete understanding of the interactions and interdependencies among energy infrastructure and other systems of critical infrastructure drives uncertainty in the total effect of the resilience enhancement options.
4. **Uncertainty in Threats and Hazards:** There continue to be large uncertainties in global climate change impacts and associated natural hazards, as well as current threats driven by human behavior (e.g., insider threat).

The importance of the electric grid in our society and the resilience of the grid to disruption have come to the forefront of society's attention. Continued research and development of new technologies, legislative and grid architectural changes, and new market models are all part of the future of grid resilience. It will take researchers, utilities, academia, and governments at all levels to move resilience of the electric power industry forward.

This page intentionally left blank

1 Introduction

The United States has one of the world's most reliable, affordable, and increasingly clean energy-based electric systems.¹ At the core of the electric system is the grid, a highly complex, engineered, and interconnected network that connects the production and delivery of power to customers. As part of the grid, transmission lines deliver high-voltage bulk electricity from the source generation facilities to substations, where the voltage is stepped down for delivery along distribution lines to commercial and residential customers. Control centers, at both the regional and local scale, serve to monitor and manage the flow of electricity. Figure 1 illustrates a general schematic of the electric power grid. In total, the grid comprises approximately 6,000 power stations and other small generation facilities; 45,000 substations connected by approximately 200,000 miles of high-voltage transmission lines; and local distribution systems that move power to customers through overhead and underground cables.²

Electricity enables and supports all critical infrastructure sectors, and our society's dependence on electricity only continues to increase. Because of its importance as a national security and economic asset, in combination with its extensiveness and visibility, the electric grid can be viewed as quite vulnerable to numerous threats and hazards. However, the design of the grid also has the potential to make it quite resilient, meaning it has the ability to minimize disruptions to energy service by anticipating, resisting, absorbing, responding to, adapting to, and recovering from a disturbance.³ For example, hardening and redundancy can be integrated into the various components and systems to reduce vulnerability and limit potential damage from a variety of threats and hazards. In addition, advanced smart-grid systems can be used to expedite information flow; remotely monitor demand, performance, and quality of service; enhance system efficiency; and improve outage detection and restoration by identifying the location and description of damaged equipment. Although it is impossible to mitigate every threat or hazard, an all-hazards approach to resilience is a logical direction for the electric industry to consider.

The electric power industry, and the grid itself, must continually adapt to the growing list of emerging threats, hazards, vulnerabilities (i.e., points of weakness), and challenges that may compromise its ability to deliver electricity to customers. The resilience of the electric grid, however, is the responsibility of multiple entities and jurisdictions, including states, utilities, and various federal regulatory bodies. Thus, electric utilities must work closely with government and other industry partners^{4,5} to apply effective risk management approaches focused on ensuring a reliable and resilient electric grid, which can ensure the continuing operation and/or quick recovery and restoration of critical services to customers when power disruptions occur, regardless of their cause.

¹ DOE EPSA (Office of Energy Policy and Systems Analysis), 2015, *Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure* (April).

² The Chertoff Group, 2014, *Addressing Dynamic Threats to the Electric Power Grid through Resilience*, Washington, D.C. (November).

³ The Chertoff Group, 2014.

⁴ Ibid.

⁵ Barrett, J.M., J. Harner, and J. Thorne, 2013, *Ensuring the Resilience of the U.S. Electrical Grid*, Lexington Institute (January).

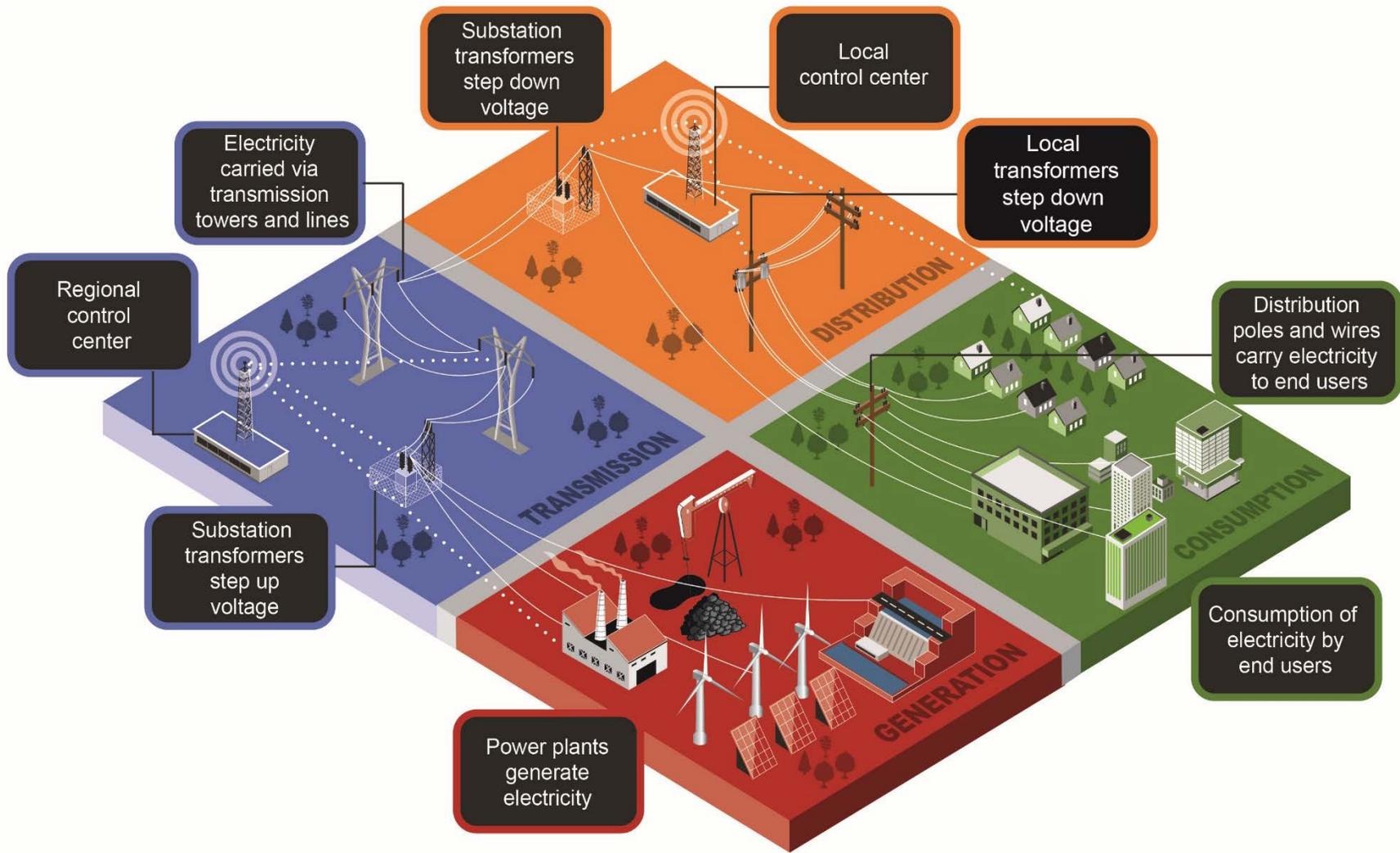


Figure 1 General Schematic of the Electric Power Grid

States and utility companies are at the front lines of assuring electric system resilience. This report summarizes how states and local utility companies are approaching all-hazards resilience in planning, construction, operations, and maintenance of the electric system. The remainder of this report contains findings and insights from stakeholders and experts involved with the day-to-day mission of ensuring electricity system resilience. As much of this work is based on discussions and observations, these insights are not conclusive. Rather, representing the views of the individuals and institutions charged with maintaining and operating the electric system on a daily basis, these insights are observational and suggestive of developing areas and topics for further exploration.

Presented first are the primary data sources used to gather the information and research included in this report. Next, this report describes the wide range of threats, hazards, and vulnerabilities faced by the electric power industry, followed by some of the most common resilience enhancement options available for and applied by electric utilities. Finally, this report identifies some of the challenges and gaps that utilities currently face when addressing resilience.

This page intentionally left blank

2 Information and Data Sources

A variety of governmental, industry, and trade associations are involved in increasing resilience of the electric grid. Each has a unique perspective and different mechanisms upon which it can influence electric system resilience. Information collected to inform this report was gathered through interviews with utility and utility contractors, discussions with industry associations, and research of publicly available resources. Table 1 expands upon the different data sources and provides a short description on each of their roles in resilience of the electric grid. For additional information on data sources, see Appendix A.

Table 1 Descriptions of Data Sources and Their Roles in the Resilience of the Electric Grid

Data Source	Role in Electric Grid Resilience
Electric Utilities and Utility Contractors	Implementers of resilience enhancement options. These entities plan for known threats and hazards, build and retrofit the infrastructure to withstand the threats and hazards, and respond after a disaster to restore the system and operational status.
Regulatory Agencies	
North American Electric Reliability Corporation	NERC’s primary focus is on reliability, which is a complement to resilience. Measures that are implemented to increase reliability can also impact resilience (withstand, respond, and recover after a severe event). NERC also promulgates and enforces the CIP mandatory standards.
Federal Energy Regulatory Commission	Independent agency that regulates the interstate transmission of electricity, natural gas, and oil. Provides oversight to NERC.
Industry Organizations	
National Association of State Energy Organizations	A nonprofit association for the governor-designated energy officials from each of the 56 states and territories. The primary role of the NASEO is to identify emerging issues relevant to the state and territory energy offices and to collect, analyze, and disseminate this information to educate members and others. It also provides direct technical assistance to States on comprehensive strategic energy planning and energy assurance, which address energy emergency responses and mitigating Energy Sector risk by investments in resilience.
National Association of Regulatory Utility Commissioners	A non-profit organization that represents the state public utility commissions (PUCs) who regulate energy, telecommunications, water, and transportation utilities. Their mission is to serve in the public interest by improving the quality and effectiveness of public utility regulation. It also provides direct technical assistance to state PUCs.
Electric Power Research Institution	A non-profit organization that conducts research and development relating to the generation, delivery, and use of electricity. Their research focuses in part on resilience of electric power systems.
Edison Electric Institute	An association that represents all U.S. investor-owned electric companies that ensure their success by advocating public policy, expanding market opportunities, and providing strategic business information.

Table 1 (Cont.)

Data Source	Role in Electric Grid Resilience
Seminal Work	
President’s Climate Action Plan (2013)	A plan intended to guide the nation toward the goal of reducing carbon emission by 17% by 2020. Actions items included conducting a Quadrennial Energy Review by the White House Domestic Policy Council and Office of Science and Technology Policy, supported by a Secretariat established at the Department of Energy, and involving the robust engagement of federal agencies and outside stakeholders.
Quadrennial Energy Review (2015)	First report focused on infrastructure challenges. It identified the threats, risks, and opportunities for U.S. energy and climate security, enabling the federal and state governments to translate policy goals into a set of analytically based, clearly articulated, sequenced and integrated actions, and proposed investments over a 4-year planning horizon.

3 Key Electric Grid Threats, Hazards, and Vulnerabilities

In general, threats and hazards can be viewed as anything that can disrupt or impact a system. Hazards are typically associated with natural events; threats are generally linked to the actions of humans. Vulnerabilities are considered points of weakness that exist within a system that increase their risk and susceptibility to adverse effects. Many threats and hazards to critical electricity infrastructure are universal (e.g., physical and cyber attacks), while others vary by geographic location and time of year (e.g., hurricanes, earthquakes, and snow storms). Threats also range in frequency of occurrence, from highly likely (e.g., weather-related events) to events less likely to occur (e.g., electromagnetic pulse). For additional details related to specific electric grid threats, hazards, and vulnerabilities, see Appendix B.

When fully considering the expansive array of threats and hazards and likelihood, combined with the possible range of severity, the resulting consequences of any event can also vary significantly and extend well beyond its immediate vicinity. On the basis of discussions with the utilities, as well as research, common issues and problems were identified regardless of source. Table 2 displays the different identified threats, hazards, and vulnerabilities grouped into three general categories: natural hazards; direct intentional threats; and other threats, hazards, and vulnerabilities. Overall, the most critical threats, hazards, and vulnerabilities to the electric distribution system are related to increased extreme weather and climate change and the aging of the infrastructure itself.

Table 2 Identified Threats and Hazards against and Vulnerabilities of Electric Infrastructure

Natural Hazards		Direct Intentional Threats		Other Threats, Hazards, and Vulnerabilities	
	Ice, snow, and extreme cold weather		Physical attacks		Geomagnetic and electromagnetic pulses
	Thunderstorms, tornadoes, and hurricane-force winds		Cyber attacks		Aging infrastructure
	Storm surge, flooding, and increased precipitation		---		Capacity constraints
	Increasing temperature and extreme hot weather		---		Workforce turnover and loss of institutional knowledge
	Earthquakes		---		Human error
	---		---		Dependencies and supply chain interruptions

Four general stages make up the electric power grid: generation, transmission, distribution, and consumption (illustrated in Figure 1). (Note: In all figures and tables, primary threats, hazards, and vulnerabilities are indicated in black font, and secondary are indicated in gray italics.) Depending on the stage, the diverse variety of threats, hazards, and vulnerabilities can have different impacts on system components. In general, generation refers to the production of electricity at power plants and the supply chain required to operate the facility. The key threats, hazards, and vulnerabilities associated with the electric power generation are illustrated in Figure 2, with further information and description provided in Table 3. Subject matter experts (SMEs) assisted in categorizing the key hazards and vulnerabilities into primary and secondary categories. Primary threats, hazards, and vulnerabilities have the highest frequency and severity of consequences; secondary ones occur or affect to a lesser degree. For industrial users, operations often require higher voltage power. Overall, power plants are designed and built to withstand the common natural hazards within the region they exist. However, impacts can be significantly amplified if a power plant is subjected to a uniquely intensive incident (e.g., 500-year storm) or regionally rare event (e.g., earthquake in the Midwest) that was not initially considered. There are different types of power generating stations, or power plants, that utilize a diverse range of fuel sources, including fossil fuels by thermal plants (e.g., coal, natural gas, petroleum), renewable fuels (e.g., solar, wind, biomass), and hydroelectric power. These fuel types have different characteristics that lead to further varying impacts, depending on the threat, hazard, or vulnerability of interest.

The electricity generated at power plants feeds into the transmission stage of the grid, which includes substations, towers, high-voltage power lines, and regional control centers. The key threats, hazards, and vulnerabilities associated with the electric power transmission are illustrated in Figure 3; further information and description are provided in Table 4. Within this stage, substations consist of transformers that step up or step down voltage to a level suitable for transmission. Step-up substations receive the power from the power plants and use transformers to increase voltage and transport electricity long distances; step-down substations, which are typically located at switching points within the grid, lower the voltage to serve as a source for distribution substations. The transmission towers and lines are the infrastructure that supports the movement of high-voltage electricity long distances. Transmission towers, which are generally constructed of steel, aluminum, or a combination, are generally tall (i.e., 49 to 180 feet [15 to 55 meters]) and serve to keep high-voltage lines away from their surroundings and from each other. Their shape (e.g., lattice, pole, H-frame, etc.) depends on a number of variables, including, but not limited to, age, required clearances, and ability to establish necessary foundations. Transmission lines are commonly made of copper, aluminum, aluminum-steel composites, or ceramic fibers in a matrix of aluminum. Overall, the design, construction, and span lengths for transmission towers and lines are highly dependent on regional weather and terrain. Finally, transmission control centers are used to house or access the information technology (IT) systems that monitor and control electric power movement along the regional-scale transmission assets. More specifically, operators at the control center are responsible for monitoring the flow of electricity within the system through electronic devices located at the generating plants, substations, and on transmission lines. The control center, in turn, relays messages to the generating plants to either increase or decrease their generation, thereby matching the amount of electricity needed at any given moment. An imbalance can cause a grid failure.

The distribution system carries and delivers electric power to the consumer, or end user, at appropriate voltages. The typical components of the distribution system include substations, pole, lower-voltage power lines, and local control centers. The key threats, hazards, and vulnerabilities associated with the electric power distribution are illustrated in Figure 4; further information and description are provided in Table 4. Electricity from the transmission system enters distribution substations, which further step down the voltage for distribution to the end users. Distribution lines are used to carry the stepped-down power to the end users and are similar to transmission lines in terms of construction. Distribution poles are typically constructed of wood, concrete, steel, or a composite material and are generally shorter (i.e., 39 feet [12 meters]) than transmission towers. As a result, they tend to be more susceptible to the impacts from strong winds, falling trees and branches, and ice storms.

The consumption phase includes the wide range of end users, from industrial facilities, to commercial facilities, to residential homes and more, which consume electricity from the grid. The key threats, hazards, and vulnerabilities associated with electric power consumption are illustrated in Figure 5; further information and description are provided in Table 5. Many industrial facilities have their own substation(s) to reduce the incoming voltage from the distribution lines or transmission lines, but still maintain the desired level of electric power to support functionality. For commercial and residential consumers, local transformers, which can be pole or pad mounted, further step down voltage for final delivery to end user meters that track actual power usage. In many cases, the utility provider manually reads meters to determine monthly usage; however, utilities are increasingly deploying automated smart meters that allow for two-way communication between the utilities and end users via smart-grid technology. This technology allows end users to have a more transparent view on their usage so they can make more informed decisions on when and how to use electric power. It allows utilities to save money because they do not need to physically read meters. Further, it provides faster outage responses and enables a range of potential new services to the customer.

Primary threats, hazards, and vulnerabilities: highest frequency and severity of consequences

Secondary threats, hazards, and vulnerabilities: occur at a lesser frequency or severity of consequence

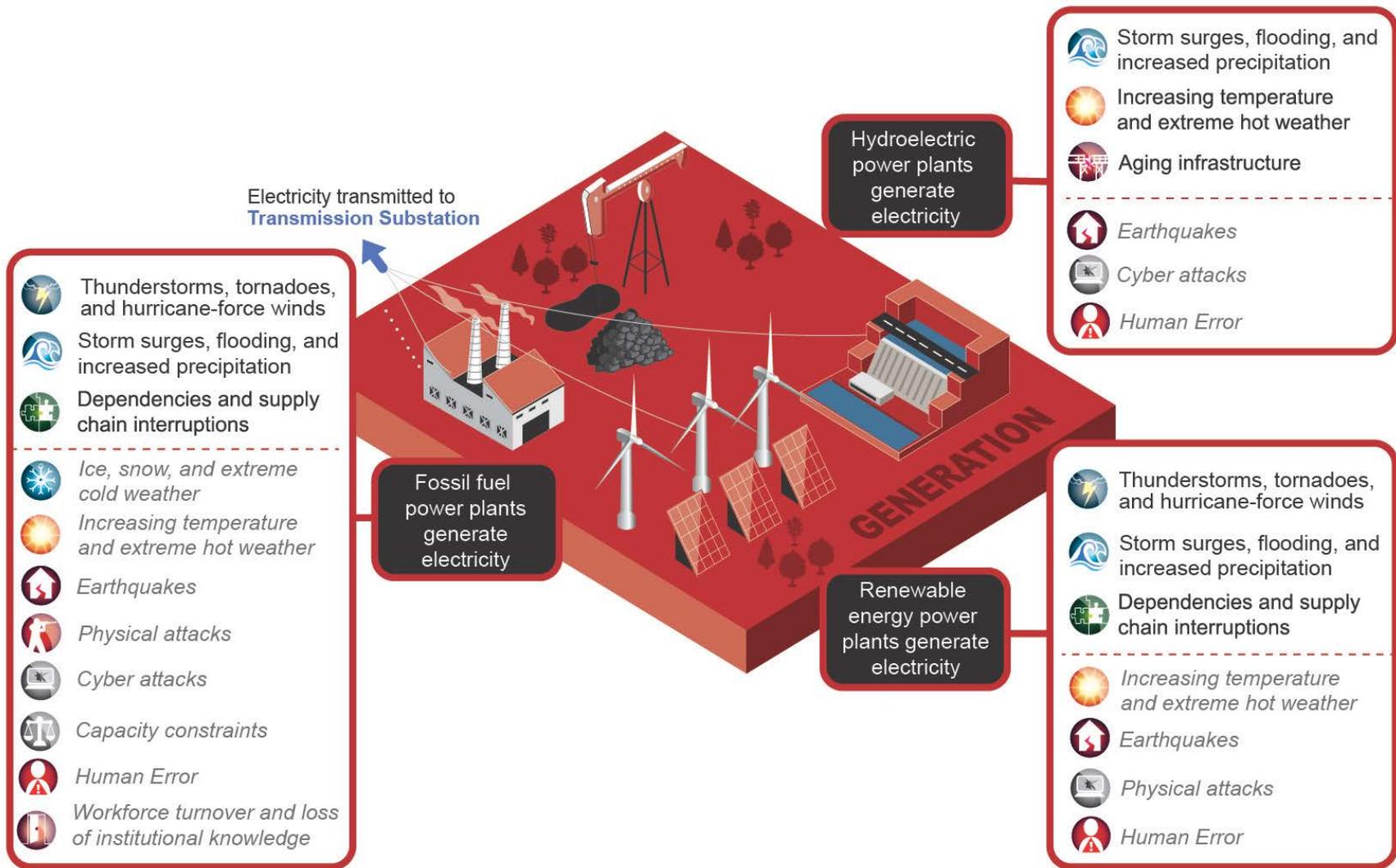


Figure 2 Electric Power Generation: Key Primary and Secondary Threats, Hazards, and Vulnerabilities (Note: black font indicates primary; gray italics indicates secondary)

Table 3 Electric Power Generation: Further Information for Key Primary and Secondary Threats, Hazards, and Vulnerabilities (primary in black font; secondary in gray italics)

Generation		
System Subcomponent	Description	
Fossil Fuel Power Plants		
Primary	Thunderstorms, Tornadoes, and Hurricane-Force Winds	Strong winds, hail, flying debris, and lightning from severe weather can damage facility buildings and exposed infrastructure elements.
	Storm Surges, Flooding, and Increased Precipitation	In coastal areas, storm surge and wave action can infiltrate, damage, and flood facility buildings and infrastructure elements. Increased precipitation intensifies the frequency, intensity, and duration of flooding, which can also lead to saturated soil conditions and weakened foundations of infrastructure elements.
	Dependencies and Supply Chain Interruptions	Fossil fuel power plants depend on transportation networks (e.g., roads, pipelines, rail, waterways, etc.) to bring fuel and raw materials to the facilities. They also rely on water for cooling.
Secondary	<i>Ice, Snow, and Extreme Cold Weather</i>	<i>Cold temperatures can be dangerous for personnel and stress facility equipment (not designed to withstand such extremes). Crippled transportation networks and an extra demand for heating gas or oil can also put a facility's fuel source delivery at risk. Certain fuel sources (e.g., coal) can freeze during transport or while in the storage yard, rendering them temporarily unusable.</i>
	<i>Increasing Temperature and Extreme Hot Weather</i>	<i>Increasing air and water temperatures reduce cooling efficiency, increase the likelihood of exceeding thermal effluent limits, and increase the risk of a partial or full plant shutdown. Increasing temperatures can also affect availability of cooling water (e.g., during drought).</i>
	<i>Earthquakes</i>	<i>Earthquakes, combined with associated tsunamis, aftershocks, and ground failure (e.g., liquefaction and lateral spreading), can result in flooding; physical damage to facility buildings, equipment, and infrastructure elements; and exposure of foundation piles. In addition to size of an earthquake, impact will depend on the region and how seismic considerations are addressed in facility design.</i>
	<i>Physical Attacks</i>	<i>Physical attacks against plants can range from vandalism to direct coordinated destruction of equipment and facilities to first-person shooters. Malicious actors carrying out these attacks encompass a wide range of potential offenders, including terrorist organizations, international enemy states, economically or otherwise competing nations, lone-wolf anarchists, disgruntled employees, and mischievous individuals.</i>
	<i>Cyber Attacks</i>	<i>Increased incorporation of advanced software and technology throughout the grid creates new vulnerabilities for cyber-based attacks. Cyber attacks range from adversaries wanting to exploit or steal something to terrorists or enemies attacking, taking over, and/or shutting down electric power system controls, including those at power plants.</i>
	<i>Capacity Constraints</i>	<i>With continually increasing electric power demand, some systems are having trouble maintaining the required excess capacity of 10%–15% greater than peak demand. New or expanded power plants may be required to keep up with demand and prevent outages due to limited availability of power.</i>
	<i>Workforce Turnover and Loss of Institutional Knowledge</i>	<i>High turnover rates, retirement of experienced workers, and loss of institutional knowledge create safety, capability, and continuity challenges. Training and development of new skilled personnel, which require a long lead time, are especially difficult to achieve with high turnover rates and decreasing numbers of experienced workers. Fewer skilled employees may also lead to more human errors.</i>
	<i>Human Error</i>	<i>Complex systems built and operated by humans are vulnerable to impacts resulting from or attributed to human-related mistakes or issues, which can be compounded by workforce turnover.</i>

Table 3 (Cont.)

		Generation	
		System Subcomponent	Description
Renewable Energy Power Plants			
Primary	Thunderstorms, Tornadoes, and Hurricane-Force Winds	Strong winds, hail, flying debris, and lightning from severe weather can damage facility buildings, equipment, and exposed infrastructure elements. Specifically, solar panels can be damaged by debris and wind turbines toppled by tornadoes.	
	Storm Surges, Flooding, and Increased Precipitation	In coastal areas, storm surge and wave action can infiltrate, damage, and flood facility buildings and infrastructure elements. Increased precipitation intensifies the frequency, intensity, and duration of flooding, which can also lead to saturated soil conditions and weakened foundations of infrastructure elements.	
	Dependencies and Supply Chain Interruptions	The water use and consumption by renewable energy technologies vary. While wind turbines and photovoltaic energy generation use essentially no water, some concentrated solar and biomass energy plants rely heavily on water for cooling.	
Secondary	<i>Increasing Temperature and Extreme Hot Weather</i>	<i>For those plants dependent on water for cooling, increasing air and water temperatures reduces cooling efficiency, increases likelihood of exceeding thermal effluent limits, and increases risk of a partial or full shutdown. Increasing temperatures can also affect availability of cooling water (e.g., during drought).</i>	
	<i>Earthquakes</i>	<i>Earthquakes, combined with associated tsunamis, aftershocks, and ground failure (e.g., liquefaction and lateral spreading), can result in flooding; physical damage to facility buildings, equipment, and infrastructure elements; and exposure of foundation piles. In addition to size of an earthquake, impact will depend on region and how seismic considerations are addressed in facility design.</i>	
	<i>Cyber Attacks</i>	<i>Increased incorporation of advanced software and technology throughout the grid creates new vulnerabilities for cyber-based attacks. Cyber attacks range from adversaries wanting to exploit or steal something to terrorists or enemies attacking, taking over, and/or shutting down electric power system controls, including those at renewable power generating sites.</i>	
	<i>Human Error</i>	<i>Complex systems built and operated by humans are vulnerable to impacts resulting from or attributed to human-related mistakes or issues.</i>	
Hydroelectric Power Plants			
Primary	Storm Surges, Flooding, and Increased Precipitation	Increased precipitation can lead to flash flooding and potential for dam overflow, bypass, or failure.	
	Increasing Temperature and Extreme Hot Weather	Increased air and water temperatures could affect availability of water (e.g., during drought) necessary for hydroelectric units to run at necessary capacity.	
	Aging Infrastructure	Most major dams, reservoirs, and hydroelectric plants in the United States (typically federally owned and operated) are 60 or more years old. Maintaining key features and function requires ongoing monitoring, maintenance, modernization, and rehabilitation of these structures and their component systems.	
Secondary	<i>Earthquakes</i>	<i>Earthquakes, combined with associated tsunamis, aftershocks, and ground failure (e.g., liquefaction and lateral spreading), can result in flooding and physical damage to facility buildings, equipment, dams, and infrastructure elements. In addition to size of an earthquake, impact will depend on region and how seismic considerations are addressed in facility design.</i>	
	<i>Cyber Attacks</i>	<i>Increased incorporation of advanced software and technology throughout the grid creates new vulnerabilities for cyber-based attacks. Cyber attacks range from adversaries wanting to exploit or steal something to terrorists or enemies attacking, taking over, and/or shutting down electric power system controls, including those at power plants.</i>	
	<i>Human Error</i>	<i>Complex systems built and operated by humans are vulnerable to impacts resulting from or attributed to human-related mistakes or issues.</i>	

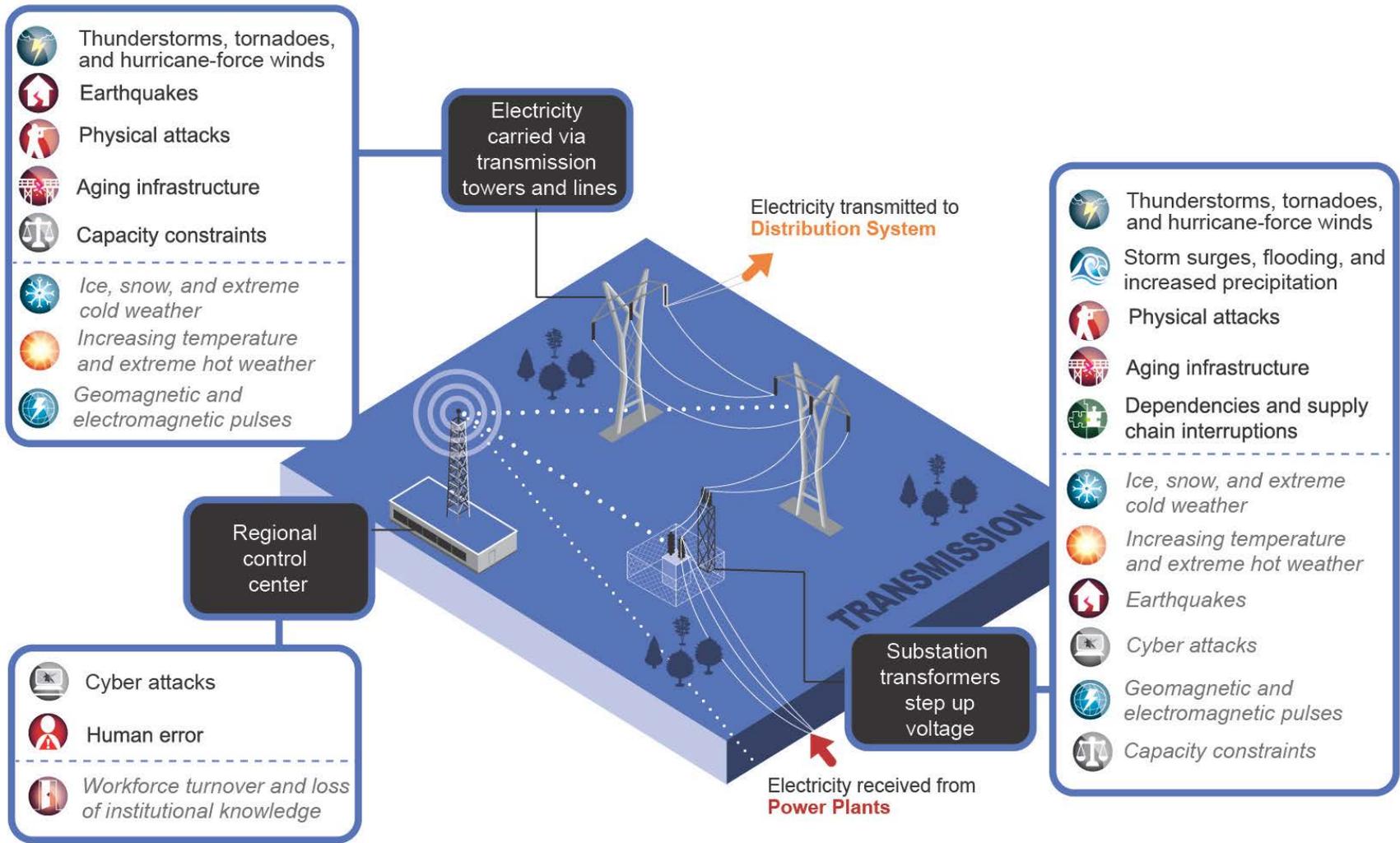


Figure 3 Electric Power Transmission: Key Primary and Secondary Threats, Hazards, and Vulnerabilities (Note: black font indicates primary; gray italics indicates secondary)

Table 4 Electric Power Transmission: Further Information for Primary and Secondary Key Threats, Hazards, and Vulnerabilities (primary in black font; secondary in gray italics)

Transmission		
System Subcomponent	Description	
Substations		
Primary	Thunderstorms, Tornadoes, and Hurricane-Force Winds	Strong winds, hail, flying debris, and lightning from severe weather can damage buildings and exposed infrastructure elements.
	Storm Surges, Flooding, and Increased Precipitation	In coastal areas, storm surge and wave action can infiltrate, damage, and flood out transmission infrastructure elements. Increased precipitation intensifies the frequency, intensity, and duration of flooding, which can also lead to saturated soil conditions and weakened foundations of infrastructure elements.
	Physical Attacks	Physical attacks against transmission substations range from vandalism to direct coordinated destruction of equipment and facilities. Malicious actors carrying out these attacks encompass a wide range of potential offenders, including terrorist organizations, international enemy states, economically or otherwise competing nations, lone-wolf anarchists, disgruntled employees, and mischievous individuals.
	Aging Infrastructure	The ages, conditions, and capacities of infrastructure vary greatly across the grid. Fully modernized or redesigned grid elements are rare, resulting in system fatigue, equipment malfunction, capacity bottlenecks, and misalignment of consumption. These lead to lost power quality, productivity, and availability.
	Dependencies and Supply Chain Interruptions	Substations are dependent upon telecommunications systems for monitoring and managing the electric grid. In addition, limited U.S. based suppliers, combined with the inherent size, complexity, and uniqueness of electric transmission system equipment, result in long lead times associated with most material assets, such as special transmission transformers.
Secondary	<i>Ice, Snow, and Extreme Cold Weather</i>	<i>Cold temperatures can stress substation equipment (not designed to withstand such extremes).</i>
	<i>Increasing Temperature and Extreme Hot Weather</i>	<i>Extreme heat causes systems and equipment to operate less efficiently and have a greater potential to malfunction. Wildfire risk is also increased.</i>
	<i>Earthquakes</i>	<i>Earthquakes, combined with associated tsunamis, aftershocks, and ground failure (e.g., liquefaction and lateral spreading), can result in flooding and physical damage to substations. In addition to size of an earthquake, impact will depend on region and how seismic considerations are addressed in facility design.</i>
	<i>Cyber Attacks</i>	<i>Increased incorporation of advanced software and technology throughout the grid creates new vulnerabilities for cyber-based attacks. Cyber attacks range from adversaries wanting to exploit or steal something to terrorists or enemies attacking, taking over, and/or shutting down electric power system controls, including those controlling and collecting data from the transmission substations. Hackers taking control of a SCADA system that gathers measurements from substations and sends out control signals to equipment could result in disrupted power flow, erroneous signals, blocked information, cut-off communication, physical damage, or more.</i>
	<i>Geomagnetic and Electromagnetic Pulses</i>	<i>These events disrupt or severely or permanently damage electronic equipment and critical grid assets. Of specific concern is a severe geomagnetic storm that can have a potentially large geographic footprint and last for many hours (or sometimes days), which would lead to considerable, wide-scale equipment damage and long-term outages to major portions of the electric grid.</i>
	<i>Capacity Constraints</i>	<i>Over-demand creates congestion points throughout the grid that can lead to curtailments, rotating blackouts, and system failures and raise the risk for larger cascading blackouts.</i>

Table 4 (Cont.)

Transmission		
System Subcomponent	Description	
Transmission Control Centers		
Primary	Cyber Attacks	Increased incorporation of advanced software and technology throughout the grid creates new vulnerabilities for cyber-based attacks. Cyber attacks range from adversaries wanting to exploit or steal something to terrorists or enemies attacking, taking over, and/or shutting down electric power system controls. Hackers taking control of a SCADA system that gathers measurements from substations and sends out control signals to equipment could result in disrupted power flow, erroneous signals, blocked information, cut-off communication, physical damage, or more.
	Human Error	Complex systems built and operated by humans are vulnerable to impacts resulting from or attributed to human-related mistakes or issues.
Secondary	<i>Workforce Turnover and Loss of Institutional Knowledge</i>	<i>High turnover rates, retirement of experienced workers, and loss of institutional knowledge create safety, capability, and continuity challenges. Training and development of new skilled personnel, which require a long lead time, are especially difficult to achieve with high turnover rates and decreasing numbers of experienced workers. Fewer skilled employees may also lead to more human errors.</i>
Towers and Lines		
Primary	Thunderstorms, Tornadoes, and Hurricane-Force Winds	Strong winds, hail, flying debris, and lightning from severe weather can damage towers, transformers, and lines, causing them to fall, break, touch, and/or short out.
	Earthquakes	Earthquakes cause physical damage to infrastructure elements, such as damage to connections in buried structures; loss, damage, collapse, or tilting of electric power towers and poles; and loss, breakage, or downing of cables and power lines. In addition to the size of an earthquake, impact will depend on the region and how seismic considerations are addressed in the tower design.
	Physical Attacks	Because they are traditionally open and cover long distances, transmission towers and lines are vulnerable to direct physical attacks ranging from vandalism to direct coordinated destruction of equipment and facilities. Malicious actors carrying out these attacks encompass a wide range of potential offenders, including terrorist organizations, international enemy states, economically or otherwise competing nations, lone-wolf anarchists, disgruntled employees, and mischievous individuals.
	Aging Infrastructure	The ages, conditions, and capacities of infrastructure vary greatly across the grid. Nationally, 70% of the transmission lines and power transformers are 25 years or older. Fully modernized or redesigned grid elements are rare, resulting in system fatigue, equipment malfunction, capacity bottlenecks, and misalignment of consumption. These lead to lost power quality, productivity, and availability.
	Capacity Constraints	Over-demand creates congestion points throughout the grid that can lead to curtailments, rotating blackouts, and system failures and raise the risk for larger cascading blackouts. Rerouting power due to aging lines can also cause overloads.

Table 4 (Cont.)

Transmission		
System Subcomponent	Description	
Secondary	<i>Ice, Snow, and Extreme Cold Weather</i>	<i>Snow and ice can weigh down trees and break branches, causing them to touch or fall on towers and lines. Ice buildup can also cause towers to collapse and lines to sag and break. Crippled transportation networks can also hinder repair efforts.</i>
	<i>Increasing Temperature and Extreme Hot Weather</i>	<i>Extreme heat creates greater peak demand for cooling, reduces current carrying capacity, increases stress, creates thermal expansion to lines (that can causes sagging and contact with tree), reduces efficiency, and creates greater potential for malfunction. Wildfire risk is also increased.</i>
	<i>Geomagnetic and Electromagnetic Pulses</i>	<i>These events disruptor severely or permanently damage electronic equipment and critical grid assets. Of specific concern is a severe geomagnetic storm that can have a potentially large geographic footprint and last for many hours (or sometimes days), which would lead to considerable, wide-scale equipment damage and long-term outages to major portions of the electric grid.</i>

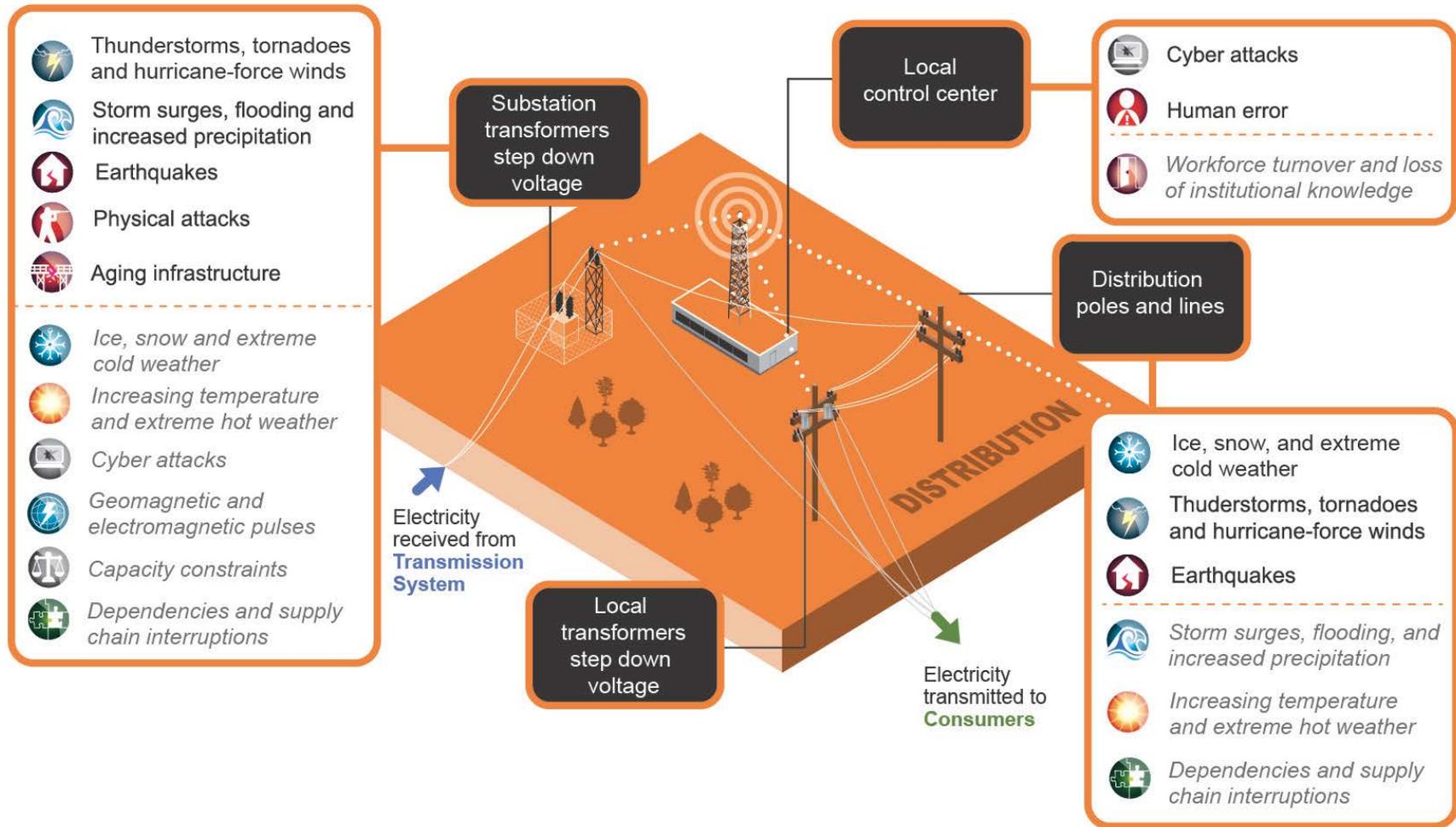


Figure 4 Electric Power Distribution: Key Primary and Secondary Threats, Hazards, and Vulnerabilities (Note: black font indicates primary; gray italics indicates secondary)

Table 5 Electric Power Distribution: Further Information for Key Primary and Secondary Threats, Hazards, and Vulnerabilities (primary in black font; secondary in italics)

Distribution		
System Subcomponent	Description	
Substations		
Primary	Thunderstorms, Tornadoes, and Hurricane-Force Winds	Strong winds, hail, flying debris, and lightning from severe weather can damage buildings and exposed infrastructure elements.
	Storm Surges, Flooding, and Increased Precipitation	In coastal areas, storm surge and wave action can infiltrate, damage, and flood distribution networks and infrastructure elements. Saltwater can be very corrosive to metal and increase the level of damage to switching and other equipment. Increased precipitation intensifies the frequency, intensity, and duration of flooding, which can also lead to saturated soil conditions and weakened foundations of infrastructure elements.
	Earthquakes	Earthquakes, combined with associated tsunamis, aftershocks, and ground failure (e.g., liquefaction and lateral spreading), can result in flooding and physical damage to facility buildings, dams, and infrastructure elements. In addition to size of an earthquake, the impact will depend on the region and how seismic considerations are addressed in the facility design.
	Physical Attacks	Physical attacks against distribution substations range from vandalism to direct coordinated destruction of equipment and facilities. Malicious actors carrying out these attacks encompass a wide range of potential offenders, including terrorist organizations, international enemy states, economically or otherwise competing nations, lone-wolf anarchists, disgruntled employees, and mischievous individuals.
	Aging Infrastructure	The ages, conditions, and capacities of infrastructure vary greatly across the grid. Fully modernized or redesigned grid elements are rare, resulting in system fatigue, equipment malfunction, capacity bottlenecks, and misalignment of consumption. These lead to lost power quality, productivity, and availability.
Secondary	<i>Ice, Snow, and Extreme Cold Weather</i>	<i>Cold temperatures can stress substation equipment (not designed to withstand such extremes). Ice storms can also damage substations, causing lines to short out.</i>
	<i>Increasing Temperature and Extreme Hot Weather</i>	<i>Extreme heat causes systems and equipment to operate less efficiently and have a greater potential to malfunction. Wildfire risk is also increased.</i>
	<i>Cyber Attacks</i>	<i>Increased incorporation of advanced software and technology throughout the grid creates new vulnerabilities for cyber-based attacks. Cyber attacks range from adversaries wanting to exploit or steal something to terrorists or enemies attacking, taking over, and/or shutting down electric power system controls, including those controlling and collecting data from the distribution substations. Hackers taking control of a SCADA system that gathers measurements from substations and sends out control signals to equipment could result in disrupted power flow, erroneous signals, blocked information, cut-off communication, physical damage, or more.</i>
	<i>Geomagnetic and Electromagnetic Pulses</i>	<i>These events disrupt or severely or permanently damage electronic equipment and critical grid assets. Of specific concern is a severe geomagnetic storm that can have a potentially large geographic footprint and last for many hours (or sometimes days), which would lead to considerable, wide-scale equipment damage and long-term outages to major portions of the electric grid.</i>
	<i>Capacity Constraints</i>	<i>Over-demand on distribution systems can lead to voltage reductions and circuit failures and raise the risk for larger cascading blackouts.</i>
	<i>Dependencies and Supply Chain Interruptions</i>	<i>Substations are dependent upon telecommunications systems for monitoring and managing the electric grid.</i>

Table 5 (Cont.)

Distribution		
System Subcomponent	Description	
Distribution Control Centers		
Primary	Cyber Attacks	Increased incorporation of advanced software and technology throughout the grid creates new vulnerabilities for cyber-based attacks. Cyber attacks range from adversaries wanting to exploit or steal something to terrorists or enemies attacking, taking over, and/or shutting down electric power system controls. Hackers taking control of a SCADA system that gathers measurements from substations and sends out control signals to equipment could result in disrupted power flow, erroneous signals, blocked information, cut-off communication, physical damage, or more.
	Human Error	Complex systems built and operated by humans are vulnerable to impacts resulting from or attributed to human-related mistakes or issues.
Secondary	<i>Workforce Turnover and Loss of Institutional Knowledge</i>	<i>High turnover rates, retirement of experienced workers, and loss of institutional knowledge create safety, capability, and continuity challenges. Training and development of new skilled personnel, which require a long lead time, are especially difficult to achieve with high turnover rates and decreasing numbers of experienced workers. Fewer skilled employees may also lead to more human errors.</i>
Poles and Lines		
Primary	Ice, Snow, and Extreme Cold Weather	Snow and ice can weigh down trees and break branches, causing them to touch or fall on poles and bring down power lines. Ice build up directly on distribution lines can also cause poles to collapse and lines to sag and break. Crippled transportation networks can also hinder repair efforts.
	Thunderstorms, Tornadoes, and Hurricane-Force Winds	Strong winds, hail, flying debris, falling trees and limbs, and lightning from severe weather can damage poles, transformers, and lines. Uprooted trees can take out underground utility lines.
	Earthquakes	Earthquakes, combined with associated tsunamis, aftershocks, and ground failure (e.g., liquefaction and lateral spreading), can result in flooding and physical damage to facility buildings, equipment, and infrastructure elements. In addition to size of an earthquake, the impact will depend on the region and how seismic considerations are addressed in the infrastructure design. Damage to transportation systems (e.g., roads, bridges, and rail lines) might also hamper delivery of equipment, crews, and supplies needed for restoration and recovery efforts.
Secondary	<i>Storm Surges, Flooding, and Increased Precipitation</i>	<i>In coastal areas, storm surge and wave action can infiltrate, damage, and flood distribution networks and infrastructure elements. Increased precipitation intensifies the frequency, intensity, and duration of flooding, which can also lead to saturated and weakened soil conditions that can cause the failure of poles and lines.</i>
	<i>Increasing Temperature and Extreme Hot Weather</i>	<i>Extreme heat creates greater peak demand for cooling, reduces current carrying capacity, increases stress, creates thermal expansion to lines (that can causes sagging and contact with tree), reduces efficiency, and creates greater potential for malfunction. Wildfire risk is also increased.</i>
	<i>Dependencies and Supply Chain Interruptions</i>	<i>Utilities depend on transportation networks to gain access to roads and areas in need of repair after an event. In addition, the same few equipment suppliers provide critical parts and components for multiple industries and utilities, which can lead to acute shortages after a large-scale event (e.g., hurricane or ice storm).</i>

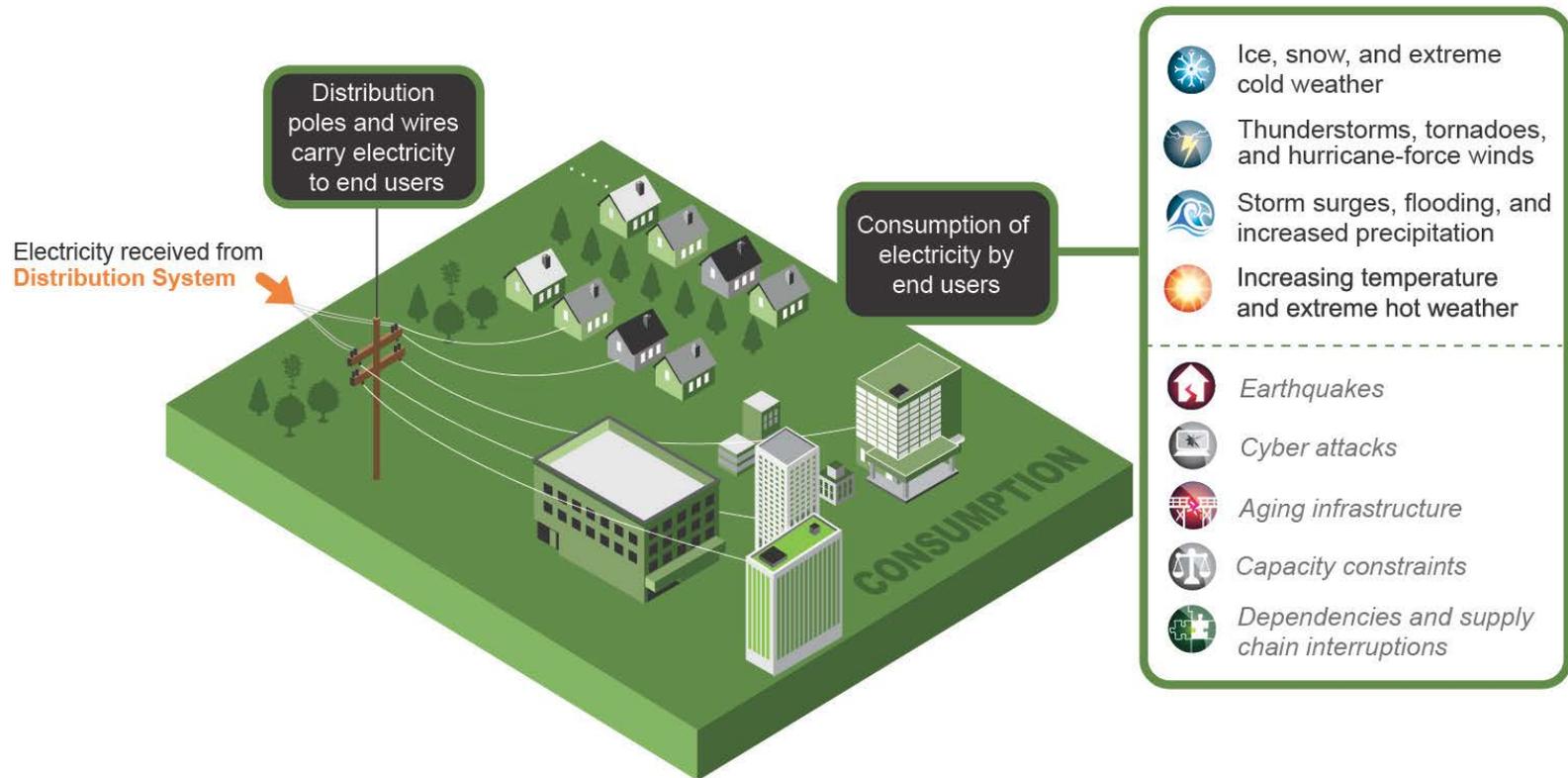


Figure 5 Consumption of Electric Power: Key Primary and Secondary Threats, Hazards, and Vulnerabilities (Note: black font indicates primary; gray italics indicates secondary)

Table 6 Consumption of Electric Power: Further Information for Key Primary and Secondary Threats, Hazards, and Vulnerabilities (primary in black font; secondary in gray italics)

Consumption		
System Subcomponent	Description	
End Users		
Primary	Ice, Snow, and Extreme Cold Weather	Snow and ice can weigh down trees and break branches, causing them to touch or fall on poles, lines, and service masts leading to end user homes, buildings, and facilities. Ice buildup can also cause poles to collapse and lines to sag and break. Crippled transportation networks can also hinder repair efforts.
	Thunderstorms, Tornadoes, and Hurricane-Force Winds	Strong winds, hail, flying debris, and lightning from severe weather can damage residential homes, commercial buildings, industrial facilities, and exposed infrastructure elements. Power will not be restored to severely damaged homes, and buildings until repair and reconstruction are completed.
	Storm Surges, Flooding, and Increased Precipitation	In coastal areas, storm surge and wave action can infiltrate, damage, and flood communities and wipe out infrastructure elements. Saltwater can be very corrosive to metal and increase the level of damage to switching and other equipment. Increased precipitation intensifies the frequency, intensity, and duration of flooding, which can also lead to saturated soil conditions and weakened foundations of infrastructure elements.
	Increasing Temperature and Extreme Hot Weather	Extreme heat causes systems and equipment to operate less efficiently and have a greater potential to malfunction. Wildfire risk is also increased.
Secondary	<i>Earthquakes</i>	<i>Earthquakes, combined with associated tsunamis, aftershocks, and ground failure (e.g., liquefaction and lateral spreading), can result in flooding, physical damage to buildings and infrastructure elements, and exposure of foundation piles. In addition to size of an earthquake, the impact will depend on the region and how seismic considerations are addressed in building and the infrastructure design.</i>
	<i>Cyber Attacks</i>	<i>Increased incorporation of advanced software and technology throughout the grid creates new vulnerabilities for cyber-based attacks. Cyber attacks range from adversaries wanting to exploit or steal something to terrorists or enemies attacking, taking over, and/or shutting down electric power system controls, including those at power plants. Automated smart meters are commonly relied on to track actual power usage and allow for two-way communication between the utilities and end users via smart-grid technology. Hackers targeting this technology could disrupt power flow, send erroneous signals, block information, cut off communication, do physical damage, or more.</i>
	<i>Aging Infrastructure</i>	<i>The ages, conditions, and capacities of infrastructure vary greatly across the grid. Fully modernized or redesigned grid elements are rare, resulting in system fatigue, equipment malfunction, capacity bottlenecks, and misalignment of consumption. These lead to lost power quality, productivity, and availability.</i>
	<i>Capacity Constraints</i>	<i>Over-demand creates congestion points throughout the grid that can lead to curtailments, rotating blackouts, and system failures and raise the risk for larger cascading blackouts. However, smart-grid technology can communicate with commercial, industrial, and residential customers about peak demand times and give them the option (or not) to reduce their electric power use during these periods (i.e., during hot summer months).</i>
	<i>Dependencies and Supply Chain Interruptions</i>	<i>Smart-grid technology depends on telecommunications systems for the monitoring and managing of end user smart meters.</i>

This page intentionally left blank

4 Resilience Enhancement Options

Resilience enhancement measures are generally applied to achieve at least one of three primary goals: (1) prevent or minimize damage to help avoid or reduce adverse events; (2) expand alternatives and enable systems to continue operating despite damage; and/or (3) promote a rapid return to normal operations when a disruption does occur (i.e., speed the rate of recovery). However, recent weather extremes, climate change impacts, physical- and cyber-security threats, and a changing workforce have added to the challenges faced by electric utilities, prompting industry to develop new multidisciplinary all-hazards approaches for managing these issues and making the grid more resilient and reliable.

Investments in resilience—defined on an all-hazards or broad systems approach that protects and mitigates against multiple threats and hazards—create projects with the potential for additional benefits beyond the primary resilience goal.⁶ As a result, investments can be more economical and may offer a return on investment, increase overall operational efficiency and possibly reduce costs, contribute to economic growth, and/or potentially decrease adverse environmental impacts. In practice, investment priorities are commonly based on analyses of outage records; condition, age, and service schedule for existing infrastructure; review of data from installed protective devices; and cost causality linkages between capital funding and the risk reduction (e.g., customer outages) obtained via that investment.^{7,8}

The remainder of this section summarizes some of the most common measures that utilities have implemented or may consider for implementation to increase the resilience of the electric grid. This information has been identified through industry input, SME consultations, lessons learned from publicly available after-action-type reports, and other publicly available data sources.

4.1 Hardening

Physically changing, or hardening, the infrastructure to make it less susceptible to damage from extreme wind, flooding, or flying debris is a common resilience measure applied by electric utilities. Hardening improves the durability and stability of infrastructure, making it better able to withstand the impacts of hurricanes and weather events without sustaining major damage, which decreases customer outages and reduces restoration times. Hardening measures usually require significant investment by the electric utilities and can include adopting new technology, installing new equipment, relocating equipment, constructing protective barriers, strengthening components, installing remote monitoring, or improving communications.^{9,10,11}

⁶ Pillon, J., 2015, Personal Communication.

⁷ Con Edison, 2016a, Personal Communication.

⁸ Central Hudson Gas & Electric Corporation, 2016a, Personal Communication.

⁹ Con Edison, 2016a.

¹⁰ PSE&G Long Island, 2016a, Personal Communication.

¹¹ DOE OE, 2010, *Hardening and Resiliency U.S. Energy Industry Response to Recent Hurricane Seasons* (August).

Hardening measures involve physical changes that improve the durability and stability of specific pieces of infrastructure—for example, elevating and sealing water-sensitive equipment, making it less susceptible to damage.¹² These elements are often applied by using a layering approach to help to protect against a single point of failure and/or to prevent wide-scale disruption to grid operations.¹³

Table 7 identifies the potential threats, hazards, and vulnerabilities that could be addressed by hardening.

Table 7 Hardening: Threats, Hazards, and Vulnerabilities Potentially Addressed

Threats, Hazards, and Vulnerabilities (primary in black font; secondary in gray italics)	
 Thunderstorms, tornadoes, and hurricane-force winds	 Storm surges, flooding, and increased precipitation
 Earthquakes	 Physical attacks
 Geomagnetic and electromagnetic pulses	 Cyber attacks
 <i>Human error</i>	

4.1.1 Wind, Ice, and Snow Protection

A common hardening practice utility providers conduct to their electric transmission and distribution systems involves upgrading cross arms, poles, cables, and structures with stronger materials and a more compact design to withstand more wind loading and damage.^{14,15,16,17} For distribution systems, this usually involves replacing wood poles with concrete, steel, or a composite material, and installing guy wires and other structural supports. These alternate materials, however, typically cost more and take longer to replace than wood poles.¹⁸ Tree wire and bundling conductors are often installed to add distribution system hardening.¹⁹ So, although many utilities routinely make these improvements during system restoration, others opt to retain their wood-based pole systems for economic reasons and potentially faster recovery times. Utilities typically upgrade transmission structure materials from aluminum to galvanized steel or

¹² GAO (United States Government Accountability Office), 2014, *Climate Change – Energy Infrastructure Risks and Adaptation Efforts*, Report to Congressional Requesters, GAO-14-74 (January).

¹³ The Chertoff Group, 2014.

¹⁴ Con Edison, 2016a.

¹⁵ PSE&G Long Island, 2016d, *PSE&G Long Island Further Strengthens Electric Grid: Resiliency Projects Protect the System from Extreme Weather*, Website.

¹⁶ DOE OE, 2010.

¹⁷ DTE Electric Company, 2014, *DTE Electric Company’s Response to MPSC Order U-17542* (February 7).

¹⁸ Keogh, M., and C. Cody, 2013, *Resilience in Regulated Utilities*, NARUC Grants and Research, with support from DOE (November).

¹⁹ Meade, 2015, Personal Communication.

concrete, with updated designs (i.e., T-shaped) enhancing the sturdiness of the structures.^{20,21} Other frequently applied hardening investments involve relocating or protecting equipment to minimize exposure to wind and trees, using hydrophobic coatings to repel water and facilitate ice removal, and/or installing breakaway devices to improve reliability.^{22,23,24,25,26}

Utility service providers can also install automatic sectionalizing fuses and reclosers to help harden overhead power lines.^{27,28,29,30} These two devices act to isolate damaged sections of lines, thereby maintaining continuity of service so that fewer customers are affected by system outages. When a fault occurs as a result of storm-related damage (e.g., a tree or branch falling or a lightning strike), sectionalizing fuses create a controlled isolation on electrical lines. These devices also allow utilities to design where breaks in the circuits will occur, thus limiting the number of affected customers. Reclosers are more complex devices that can clear temporary faults, such as a fallen tree branch that momentarily touches a line, and instantly restore service. It combines a circuit breaker that trips if an overcurrent is detected (indicating a short circuit somewhere in a section of the network), with an electronically controlled reclosing function that automatically restores power to the affected line if the fault clears itself quickly—which happens around 80 percent of the time.^{31,32} These devices result in better supply continuity to customers, faster restoration of service, and alleviation of the need to send a crew to fix the damage.³³

As an illustrative example of storm hardening, one utility has installed thousands of sectionalizing fuses and reclosers on their overhead system to isolate damage to overhead lines, so when outages occur, fewer customers are affected. These post-Superstorm Sandy initiatives are part of a \$1.3 billion investment for protecting systems from severe storms. They have already prevented outages to more than 20,000 customers in the first few months of 2016.³⁴

4.1.2 Flood Protection

Flood hardening of generating stations generally entails a combination of inundation control with the relocation or elevation of critical mechanical and electrical equipment (or entire facilities) to less vulnerable locations above the defined flood-control elevation.^{35,36} Examples of potential

²⁰ DOE OE, 2010.

²¹ Meade, 2015.

²² Con Edison, 2016a.

²³ Central Hudson Gas & Electric Corporation, 2016a.

²⁴ PSE&G Long Island, 2016a.

²⁵ DTE Electric Company, 2014.

²⁶ EPRI, 2013, *Enhancing Distribution Resiliency—Opportunities for Applying Innovative Technologies* (January).

²⁷ Con Edison, 2016a.

²⁸ Central Hudson Gas & Electric Corporation, 2016a.

²⁹ PSE&G Long Island, 2016a.

³⁰ DTE Electric Company, 2014.

³¹ ABB, 2015, *Why Use Reclosers?*

³² Barrett et al., 2013.

³³ Con Edison, 2016a.

³⁴ Ibid.

³⁵ DOE OE, 2010.

inundation protection measures that utility providers can install to help control flood water include sluice gates in the intake and discharge tunnels; submersible equipment; walls that can withstand higher flood levels; pressure-resistant/submarine-type doors to protect deep basements or structures; additional high-capacity, flood-control pumps; and new emergency generators to power flood pumps and provide additional support to the stations during an emergency.^{37,38}

In general, it is far less expensive for electric power service providers to replace transmission and distribution assets than to build and maintain flood protection (e.g., berms or levees). Some utilities, however, have protected against flood damage by elevating substations above the flood zone and relocating critical equipment and facilities to areas less susceptible to water inundation, particularly when considering the impact from storm surges.³⁹ In addition, utilities can alternately opt to replace nonsubmersible equipment (e.g., transformers and network protectors) located within flood zones with submersible equivalents.⁴⁰ In the case of network protectors, submersible units can be opened to de-energize customers' equipment that is not submersible, so that feeders supplying the network protectors will remain in service.

Some utilities have started to address flood risk and hardening, based on lessons learned during Hurricane Katrina. One company proactively began to require interconnecting customers in flood-prone areas to either install submersible electrical equipment or raise critical equipment above the ground floor. By taking these steps, not only have the potential impacts of a major flooding event on those customers' equipment been mitigated, but it also reduces the probability that the electric distribution system would be impacted by a fault current on the customers' side of the meter.⁴¹

Similar activities have also resulted due to the experiences during and after Sandy, where utilities have also begun actively and proactively to install submersible transformers and network protectors when equipment in flood-prone areas is replaced, upgraded, or newly installed. For context, during Superstorm Sandy, three coastal networks were preemptively taken out of service (i.e., Bowling Green, Fulton, and Brighton Beach). These three networks had too many 460-volt services in the flood zones, such that shutting the associated feeders down would not leave enough feeders in service to supply the remaining network load. Further, 24 additional feeders in eight other coastal networks were shut down to de-energize 460-volt services that are generally used to supply larger buildings. In addition, multiple network feeders de-energized because of faults on high-transmission voltage equipment. Post-Sandy, it took 5 days to restore service and 11 days to return to full contingency design (i.e., N-2), primarily because many network protector replacements were required. By installing submersible units that eliminate the need to replace equipment, the utilities aim to reduce these periods to 24 and 48 hours, respectively.⁴²

³⁶ Keogh and Cody, 2013.

³⁷ Con Edison, 2016a.

³⁸ PSE&G Long Island, 2016a.

³⁹ DOE OE, 2010.

⁴⁰ Con Edison, 2016a.

⁴¹ Ibid.

⁴² Ibid.

4.1.3 Buried Power Lines

Utility providers can install distribution lines underground to eliminate the susceptibility to many physical threats and hazards, including direct physical attacks and weather (e.g., wind, snow, ice, and lightning damage) that are typically experienced with overhead lines. A North Carolina utility compared 5 years of underground and overhead reliability data and found that the frequency of outages on underground systems was 50 percent less than for overhead systems. However, the average duration of an underground outage was 58 percent longer, probably because of lengthier troubleshooting and restoration times, which also translate to higher repair costs. In addition, underground wires, particularly those in coastal or flood-prone regions, are more susceptible to water intrusion and damage (e.g., saltwater corrosion) from storm surge flooding than overhead wires and possibly earthquakes.^{43,44}

There is no precise per-mile cost for underground wires, primarily because every construction project is unique due to widely varying loads, the number of customers served, and construction parameters. It has been estimated, however, that burying wires costs approximately 5–15 times the construction cost of overhead lines for larger distribution lines.^{45,46,47} As a result, many utilities perform selective undergrounding on a case-by-case basis, often in conjunction with communities and customers, to protect critical and/or susceptible circuits.^{48,49,50,51}

4.2 Security Measures

4.2.1 Physical Security

Physical security measures reduce risk through physical means or defense measures that detect and deter intrusions, attacks, and/or the effects of manmade events. Physical security measures are also important for utilities to use when protecting and limiting access to information about critical components and substations, such as engineering drawings, power flow modeling runs, and site security information, which could be useful to a potential attacker. Utilities can employ access control measures such as in-depth security checks on all employees (including contractors), badged entry and limited access areas, and surveillance and monitoring (i.e., cameras, sensors, imaging, and special detection equipment).⁵²

⁴³ DOE OE, 2010.

⁴⁴ EPRI, 2013.

⁴⁵ Meade, 2015.

⁴⁶ DOE OE, 2010.

⁴⁷ EPRI, 2013.

⁴⁸ Con Edison, 2016a.

⁴⁹ Central Hudson Gas & Electric Corporation, 2016c, *Projects*, Website.

⁵⁰ PSE&G Long Island, 2016a.

⁵¹ Keogh and Cody, 2013.

⁵² Meade, 2015.

Another common form of physical security is related to the use of reinforced buildings, barriers, and fences. Utilities can construct reinforced buildings and fences using specially designed materials, such as metal mesh, which increase protection against cutting, climbing, ramming, and pass-through, and can shield assets from offsite attacks by visually obstructing them from view. Bulletproof ballistic fiberglass laminates can further protect against a wide range of small-arms fire (i.e., bullets are imbedded, rather than ricocheted).^{53,54} Utilities can also use special materials to retrofit transformers and substation controls to protect them from geomagnetic pulse (GMP) and electromagnetic pulse (EMP) effects.

4.2.2 Cybersecurity

Cyber attacks against the electric power industry are constant and continuously evolving.⁵⁵ Cybersecurity measures help protect against and recover from these attacks. Protection measures, such as firewalls, are used by utilities to detect intrusion into systems and protect data stored by a facility. Backup capabilities, systems, and servers are common recovery and restoration measures used by service providers in the event of a successful attack.⁵⁶ While many of these measures are site or company-specific, the electric power industry has a set of mandatory, enforceable cybersecurity standards known as critical infrastructure protection (CIP) standards, which were developed and approved by the industry, North American Electric Reliability Council (NERC), and the Federal Energy Regulatory Commission (FERC). The CIP standards provide a baseline for the security of the electric grid and its assets, which are critical for continued operations of the grid. Security measures contained in the standards include the implementation of risk and security training, the identification and categorization of critical assets, the use of cyber and physical security measures to protect assets or continue operations, and the establishment of response and recovery plans.⁵⁷

Information sharing is another measure used to improve cybersecurity within the electric power industry. The U.S. Department of Homeland Security (DHS) Cyber Risk Information Sharing Program (CRISP) allows participating companies to share threat information and situational awareness tools.^{58,59} These companies can use CRISP to make near real-time, informed security decisions with regard to cyber threats. Originally formed as a partnership among the U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability, the Electric Sector Information Sharing and Analysis Center (ES-ISAC), Pacific Northwest National Laboratory, Argonne National Laboratory, and participating electric companies, CRISP invites participants to voluntarily share cyber threat data.⁶⁰ In exchange, companies receive analysis and

⁵³ Ibid.

⁵⁴ Amortex, 2015, *Fire Containment & Ballistic Protection for Critical Infrastructure from Amortex*.

⁵⁵ EPRI, 2013.

⁵⁶ Pillon, 2015.

⁵⁷ The Chertoff Group, 2014.

⁵⁸ Ibid.

⁵⁹ PSE&G Long Island, 2016a.

⁶⁰ The Chertoff Group, 2014.

information that can be used to help protect their systems.^{61,62} Many utilities participate in CRISP as well as the Multi-State Information Sharing and Analysis Center (MS-ISAC), from which they receive daily bulletins. MS-ISAC provides real-time network monitoring as well as early cyber threat warnings and advisories. Other MS-ISAC services include vulnerability identification and mitigation and incident response. Some utilities also receive cyber information from law enforcement agencies in New York and New Jersey.⁶³

In addition to following the CIP standards and sharing information with others in the industry, utilities can use modeling techniques to explore what types of cyber-attack scenarios end in them successfully withstanding the attacks and which fail. These techniques can be helpful in determining how assets can respond to the attacks that made it past the protective measures.⁶⁴

Table 8 identifies the potential threats, hazards, and vulnerabilities that could be addressed by security measures.

Table 8 Security Measures: Threats, Hazards, and Vulnerabilities Potentially Addressed

Threats, Hazards, and Vulnerabilities	
 Physical attacks	 Cyber attacks
 Human error	

4.3 Maintenance and General Readiness

A large part of the resilience for the electric grid involves maintenance of its components during day-to-day operations. Utilities conduct routine maintenance of the grid components, which includes the clearing of debris and management of vegetation around grid assets, to help minimize or prevent outages and impacts to the grid.^{65,66} Tree trimming and clearing of other vegetation from power line rights of way help prevent outages, particularly during strong storms.^{67,68} Overgrown trees and vegetation can impact both transmission and distribution lines.⁶⁹ For example, the 2003 Northeast power blackout started when a high-voltage line in Ohio brushed against overgrown tree limbs. The incident impacted around 50 million people and resulted in more than \$6 billion in losses.⁷⁰ To determine clearance standards and trim

⁶¹ Ibid.

⁶² PSE&G Long Island, 2016a.

⁶³ Ibid.

⁶⁴ EPRI, 2013.

⁶⁵ Barrett et al., 2013.

⁶⁶ EPRI, 2013.

⁶⁷ Ibid.

⁶⁸ Con Edison, 2016a; Central Hudson Gas & Electric Corporation, 2016a; PSE&G Long Island, 2016a; DOE OE, 2010; Pillon, 2015.

⁶⁹ Ibid.

⁷⁰ Barrett et al., 2013.

specifications, utilities have started to assess storm damage and associated restoration.⁷¹ These studies have identified that branches and trees falling onto power lines have larger impacts to the supply of power than growing vegetation below, and the removal of overhanging branches should be prioritized over removal of lower vegetation.⁷²

Maintenance also includes the inspection of and replacement of worn-out components, such as transmission structures and distribution poles.^{73,74} Pole inspections, which local utilities can conduct year round, are intended to identify assets in need of maintenance to prevent unscheduled or emergency maintenance. The inspections also help companies make informed decisions on prioritizing asset maintenance and upgrades based on available resources. One common inspection method is to use infrared technology; equipment is mounted onto vehicles or aircraft. Transmission lines and other components in need of maintenance often have a significantly different temperature in comparison to their surroundings, and infrared equipment can identify such instances.⁷⁵

Table 9 identifies the potential threats, hazards, and vulnerabilities that could be addressed by maintenance and general readiness measures.

Table 9 Maintenance and General Readiness: Threats, Hazards, and Vulnerabilities Potentially Addressed

Threats, Hazards, and Vulnerabilities (primary in black font; secondary in gray italics)	
 Thunderstorms, tornadoes, and hurricane-force winds	 Storm surges, flooding, and increased precipitation
 Earthquakes	 Aging infrastructure
 Human error	 Workforce turnover and loss of institutional knowledge
 Dependencies and supply chain interruptions	 <i>Ice, snow, and extreme cold weather</i>
 <i>Increasing temperature and extreme hot weather</i>	 <i>Capacity constraints</i>

⁷¹ EPRI, 2013.

⁷² Central Hudson Gas & Electric Corporation, 2016a.

⁷³ Barrett et al., 2013.

⁷⁴ DOE OE, 2010.

⁷⁵ Ibid.

4.4 Modernization, Control Enhancements, and Smart-Grid Technology

Utility companies across the country, such as DTE Electric Energy and others, are implementing smart-grid technologies to improve performance, security, and efficiency.^{76,77,78,79}

Implementation of the smart grid includes the use of sensors on transmission and distribution assets to provide real-time, two-way communications between the utilities and customers. Data about consumer demand are sent from the customers to the utilities, and electric power is sent from the utilities to the customers. Computing power is also required to be able to store and analyze the information being collected. The real-time knowledge on precise demand, supply flows, and energy loss throughout the system is important because electricity from the grid cannot currently be stored—it is continuously generated, transmitted, and used.⁸⁰ The collection of data from the customer allows utilities to balance supply and demand, therefore increasing the efficiency of asset use (e.g., power plants and distribution substations) and potentially offsetting the need for additional power generation or construction of new assets.^{81,82,83}

In addition, data collection by the utilities allows for the identification of anomalies in the system. The Energy Information Administration (EIA) determined that \$20 billion in losses to the economy (in 2005) was due to loss of electricity during transmission and distribution operations. Studies performed by the Electric Power Research Institution (EPRI) (in 2001) estimated the cost of power disturbances across all business sectors in the United States at between \$104 billion and \$164 billion a year as a result of outages, with another \$15 billion to \$24 billion due to power quality phenomena⁸⁴ (e.g., harmonic distortions and voltage fluctuations, feeder voltage regulations, and lightning strikes). The more rapid detection of anomalies and failures by the utilities will allow for faster response and will, therefore, help reduce such losses and help minimize adverse effects from system failures.⁸⁵ Some utilities using smart-grid technologies in advanced metering demonstration projects are seeing reductions in their peak load by more than 40 percent. Further, customers are saving an average of \$200 during the project period, and outage times following storms have decreased.⁸⁶

Customers also play a role in energy efficiency. Smart-grid technology can communicate with both industrial and household customers about peak demand times and give them the option to reduce their electric power use during these times. The benefit to the customer is the implementation of variable costs based on time of day; electric power usage during nonpeak times costs a customer less than power used at the time of highest demand. In 2008, DOE's

⁷⁶ DTE Electric Company, 2014.

⁷⁷ Central Hudson Gas & Electric Corporation, 2016a.

⁷⁸ DOE, 2008, *The Smart Grid: An Introduction*.

⁷⁹ Con Edison, 2016a.

⁸⁰ Barrett et al., 2013.

⁸¹ DOE, 2008.

⁸² Barrett et al., 2013.

⁸³ DOE, 2008.

⁸⁴ EPRI, 2001, *The Cost of Power Disturbances to Industrial and Digital Economy Companies* (June).

⁸⁵ Barrett et al., 2013.

⁸⁶ DOE OE-NASEO, 2012.

Office of Electricity Delivery and Energy Reliability (OE) sponsored a smart-grid primer, meant to convey concepts associated with the smart grid in layman's terms. According to that primer, "10% of all generation assets and 25% of distribution infrastructure are required less than 400 hours per year, roughly 5% of the time." More evenly distributed energy usage means a more efficient system.⁸⁷

The real-time, two-way communication combined with sectionalizing switches, allows utilities to isolate parts of the system that are failing and maintain or restore power to the surrounding areas.^{88,89} Entergy used smart-grid technology to quarantine an area experiencing loss of power and, therefore, prevent the power outage from impacting a larger area during Hurricane Gustav in 2008. Entergy had the advantage of real-time monitoring of the situation through the smart grid.⁹⁰ Other utilities are installing sectionalizing switches to their underground coastal networks in areas most susceptible to corrosive saltwater flooding. As part of this installation process, separate flood areas are being created within the grid to allow isolation of specific, smaller areas and to help prevent expansive outages.⁹¹

The installation of all smart-grid-related technologies requires utilities to spend a significant amount of money. For instance, replacing current \$40 analog meters with smart meters can cost up to \$200 each.⁹² Therefore, some utilities are converting their existing devices, such as disturbance fault recorders and relays, to act like phasor measurement units.⁹³ The benefits of utilities using smart-grid technologies include the ability to anticipate and prevent some disruptions through the use of continuous self-assessments, to fix problems quickly, and to support the growing digital economy by providing varying grades of power quality. Utilities can also save money from not having to physically read meters, provide faster outage responses, and enable a range of potential new services to the customer. Different sources of power generation, including distributed generation, renewables, energy storage, and demand response, can also be incorporated through the smart grid.⁹⁴ The DOE has worked with industry to develop the Smart Grid Maturity Model (SGMM). The SGMM is a self-assessment tool that provides utilities with suggested activities, investments, and best practices to incorporate smart-grid technologies into their systems.⁹⁵

While the smart grid is associated with many benefits, there are a few challenges to the integration of the technologies into current systems. Incorporating the new technologies can be difficult from a technical aspect and also from a financial standpoint. In addition, the IT built into the smart grid exposes the system to cybersecurity and privacy concerns⁹⁶; thus, security issues must be considered upon implementation.

⁸⁷ DOE, 2008.

⁸⁸ Barrett et al., 2013.

⁸⁹ Con Edison, 2016a.

⁹⁰ DOE, 2008.

⁹¹ Con Edison, 2016a.

⁹² Barrett et al., 2013.

⁹³ DOE OE-NASEO, 2012.

⁹⁴ DOE, 2008.

⁹⁵ Ibid.

⁹⁶ DOE EPSA, 2015.

Modernization efforts by utilities can include options that are not technology related, such as improving real-time monitoring and rerouting. For example, near the Chicago downtown area, the use of superconductive cable, which allows for an increased supply through a smaller cable, is being proposed. Nitrogen cools the cables and lowers the resistance levels. The utilities can install superconductive cable underground, which is beneficial for areas with limited space for aboveground lines.⁹⁷

Table 10 identifies the potential threats, hazards, and vulnerabilities that could be addressed by modernization, control enhancements, and smart-grid technology measures.

Table 10 Modernization, Control Enhancements, and Smart-grid Technology: Threats, Hazards, and Vulnerabilities Potentially Addressed

Threats, Hazards, and Vulnerabilities (primary in black font; secondary in gray italics)			
	Ice, snow, and extreme cold weather		Thunderstorms, tornadoes, and hurricane-force winds
	Cyber attacks		Aging infrastructure
	Human error		<i>Capacity constraints</i>

4.5 Diversified and Integrated Grid

The electric power grid continues to evolve as technology advances and distributed energy generation resources are increasingly deployed. New technologies are increasing the optimization of the grid and the operators’ ability to detect and troubleshoot problems.⁹⁸ The architecture of the grid is moving away from the tradition hub and spoke model, to a more integrated grid with multiple generation options. Distributed generation resources include, but are not limited to, natural gas-fueled generators, combined heat and power plants, electricity storage, wind generations, electric vehicles, and solar photovoltaics on rooftops.⁹⁹ Figure 6(a) shows the current architecture of the power grid; Figure 6(b) depicts a diversified and integrated grid.

⁹⁷ Meade, 2015.

⁹⁸ DOE EPSA, 2015.

⁹⁹ EPRI, 2014a, *The Integrated Grid: Realizing the Full Value of Central and Distributed Energy Resources*, Technical Results (February).

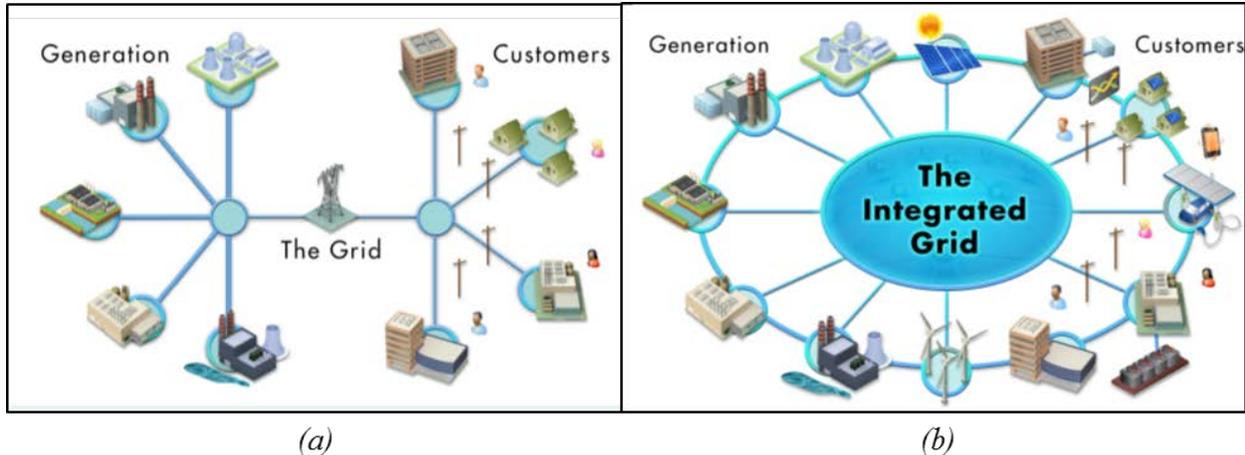


Figure 6 (a) Current Electric Grid (b) Diversified and Integrated Electric Grid¹⁰⁰

The integration of distributed generation resources into the grid poses a few challenges for the electric power suppliers and the distributed generation resource providers. For instance, the grid's original design did not consider the accommodations needed for incorporating distributed generation resources in high quantities or their variability and intermittency, all while simultaneously maintaining its current capabilities. Therefore, the integration of these distributed resources should be considered by the electric power supplier in the planning and operation of the grid.¹⁰¹ There are benefits to distributed generation as well, especially the more consistent sources of generators, such as gas-fueled generators or cogeneration, or combined heat and power plants. For example, the use of cogeneration capability provides distributed resource generation and a higher efficiency in the thermal cycle.¹⁰² A large housing development known as Co-op City in the Bronx, maintained electric power when the winds brought down the surrounding electric grid during Hurricane Sandy.¹⁰³

Utilities can use technology to control the generation of electricity centrally from multiple alternative sources. These sources can aggregate and economically optimize the dispatch of distributed generation resources. This capability is critical to the efficient and effective integration of variable power sources into the grid.¹⁰⁴ The current reliability technologies and reporting have grown from an era of more or less steady power generation supply that can be controlled from the generation plant. Variable power sources contain a source of uncertainty in generation amount and timing. Utilities need to include mitigation measures to address that variability in solutions to effectively incorporate these sources.

¹⁰⁰ Ibid.

¹⁰¹ EPRI, 2014b, *The Integrated Grid Phase II: Development of a Benefit-Cost Framework*, Technical Results (May).

¹⁰² Pillon, 2015.

¹⁰³ Alliance to Save Energy, 2012, *CHP Kept Schools, Hospitals Running Amid Hurricane Sandy* (December).

¹⁰⁴ Barrett et al., 2013.

In their 2014 report on the value of central and distributed energy sources, EPRI introduced a case summary on Germany’s integration efforts with respect to incorporating distributed energy resource (DER) technologies. Germany was at a disadvantage from the start, as they did not consider the integration of a large volume of DER into the existing power system. Lessons learned from Germany’s experiences include variable disruptions into normal system planning and concerns from customers on maintaining regulated frequency and voltage expected from consumers.¹⁰⁵ DOE EPSA noted that utilities in areas with significant levels of distributed solar generation penetration (e.g., California and Hawaii) have faced operational issues as far as two-way power flows associated with these behind-the-meter technologies.¹⁰⁶

Another option utilities have for diversification of the grid includes the development and deployment of microgrids. Utilities installing community microgrids aim to supply electricity to groups of businesses and consumers in specific geographic areas using many different sources of power generation.¹⁰⁷ In addition, large-scale microgrids can provide frequency control reserves and reduce or offset substation and feeder investments.¹⁰⁸

Utilities are also considering energy storage to manage demand.¹⁰⁹ Prior to large-scale interest in variable power systems, common sources of power storage are to pump water uphill to fill a large water reservoir that can be released later to power the generators in a dam, or to pump air into an underground cavern and compress it to more than 1,000 pounds per square inch, then release it the next day to spin a turbine.¹¹⁰ Interest has been expanding into large battery units to store excess electricity for release into the grid when needed.

Table 11 identifies the potential threats, hazards, and vulnerabilities that could be addressed by diversified and integrated grid measures.

Table 11 Diversified and Integrated Grid: Threats, Hazards, and Vulnerabilities Potentially Addressed

Threats, Hazards, and Vulnerabilities	
 Ice, snow, and extreme cold weather	 Thunderstorms, tornadoes, and hurricane-force winds
 Storm surges, flooding, and increased precipitation	 Increasing temperature and extreme hot weather
 Earthquakes	 Capacity constraints
 Human error	 Dependencies and supply chain interruptions

¹⁰⁵ EPRI, 2014b.

¹⁰⁶ DOE EPSA, 2015.

¹⁰⁷ Meade, 2015.

¹⁰⁸ DOE EPSA, 2015.

¹⁰⁹ PSE&G Long Island, 2016a.

¹¹⁰ Barrett et al., 2013.

4.6 Redundant Capabilities, Backup Equipment, and Inventory Management

Redundancy is a key component of resilience. Redundancy, however, can be expensive and is used sparingly because the investment in and upkeep of redundant systems and material can run contrary to sustainable business models for utilities.¹¹¹ Nevertheless, utilities do maintain some amount of redundancy in their systems according to their risk. Utilities can approach redundancy in various ways, including (1) maintaining spare equipment (such as distribution poles, wires, cables, switches, and distribution transformers) for rapid repair when issues arise or (2) having priority sourcing agreements in place with manufacturers or suppliers. The latter can prescribe, among other incentives, guaranteed lead times, in exchange for the supplier being the utility's primary or exclusive supplier.^{112,113} The availability and amount of resources maintained in the inventory depend on the type, size, and frequency of events that a company usually faces.¹¹⁴

Representatives from multiple utilities commented on their equipment inventory policies. One utility stores bulk material in locked containers specifically in reserve for use following large storms; these materials can supply an expanded workforce for several days. A restoration effort that extends beyond several days with a significantly expanded workforce could require some level of restocking before the restoration work is complete.¹¹⁵ Another utility noted that they increase inventories of commonly used transmission and distribution hardware prior the summer storm season to the levels used to restore service following Hurricane Gloria. Special arrangements are made with suppliers to maintain higher inventory levels needed to support the response to a major storm or hurricane.¹¹⁶

An inventory of spare parts is not always a feasible model, especially for transmission system material assets (e.g., high-voltage transformers and long-distance cable systems). Utilities do not stockpile such assets because of their high cost, long lead times, and utility-specific designs. A broader use of interchangeable parts could enable even small stockpiles of spare parts to cover a larger number of critical pieces of equipment to mitigate against the impact of long lead times associated with procurement of those large, nonstandard assets, as they frequently come from overseas sources.¹¹⁷ The DOE recently announced—as part of its Grid Modernization Lab Consortium (GMLC) effort¹¹⁸—a project focusing on delivering recommendations for the population, the location, and operation of a strategic transformer reserve, as a measure to mitigate against this vulnerability. Currently, many utilities participate in regional mutual assistance groups that can facilitate the procurement of a temporary, imperfectly fitting solution. In these cases, the temporary units allow reestablishment of system operations at a reduced capacity or load until a perfect design fit option can be acquired.¹¹⁹

¹¹¹ Ibid.

¹¹² DOE OE, 2010.

¹¹³ Meade, 2015.

¹¹⁴ Ibid.

¹¹⁵ Central Hudson Gas & Electric Corporation, 2016a.

¹¹⁶ PSE&G Long Island, 2016a.

¹¹⁷ Barrett et al., 2013.

¹¹⁸ DOE, 2016, *DOE Grid Modernization Laboratory Consortium – Awards*.

¹¹⁹ Meade, 2015.

Another common resilience activity that utilities can do involves the purchasing/leasing of portable generators. These units enable the temporary restoration of grid service by circumventing damaged equipment, allowing time for repairs.¹²⁰ Utilities exploring the option of portable generators should consider the amount of load that can be carried with that generator, how long it will last, and how much fuel is maintained to supply that generator. Companies should have source agreements with fuel suppliers to bring in extra fuel supply during an emergency. If a large-scale event occurs, it may be untenable for the fuel supplier to deliver the fuel, so utilities should have plans for alternative sources of fuel.¹²¹ The proposed Tres Amigas project in eastern New Mexico, for example, looks to mitigate against a large-scale event through the sharing of generated power across a large loop of multi-gigawatt-capacity superconducting cable for the Eastern, Western, and Texas interconnections, which will allow the excess capacity within one system to flow to the affected system.¹²²

Utilities can also use mobile transformers and substations to temporarily replace damaged assets. “A mobile substation includes a trailer, switchgear, breakers, emergency power supply, and a transformer with enhanced cooling capability. These units enable the temporary restoration of grid service while circumventing damaged substation equipment, allowing time to repair grid components. Mobile transformers are capable of restoring substation operations in some cases within 12–24 hours.”¹²³

Finally, with the increasing interdependence between communications and electric power, redundancy in communications systems is also essential to ensuring continuity of operations. Some utilities have expanded satellite communications capabilities with mobile satellite trailers that can be deployed to field staging areas and include full capabilities for email, Internet, outage management systems, voice-over Internet protocol telephones, and portable and fixed satellite phones. Others have redundant dedicated fiber-optic lines to enable continued operations.^{124, 125}

Table 12 identifies the potential threats, hazards, and vulnerabilities that could be addressed by redundant equipment, backup, and inventory management measures.

¹²⁰ DOE OE, 2010.

¹²¹ Pillon, 2015.

¹²² Barrett et al., 2013.

¹²³ DOE OE, 2010.

¹²⁴ Ibid.

¹²⁵ Meade, 2015.

Table 12 Redundancy, Backup Equipment, and Inventory Management: Threats, Hazards, and Vulnerabilities Potentially Addressed

Threats, Hazards, and Vulnerabilities (primary in black font; secondary in gray italics)	
 Ice, snow, and extreme cold weather	 Thunderstorms, tornadoes, and hurricane-force winds
 Storm surges, flooding, and increased precipitation	 Increasing temperature and extreme hot weather
 Earthquakes	 Aging infrastructure
 Capacity constraints	 Human error
 Dependencies and supply chain interruptions	 <i>Physical attacks</i>

4.7 Mutual Aid Programs

Mutual aid programs can be invaluable during the response and recovery from a major disaster. In March 2004, the Federal Emergency Management Agency (FEMA) released the National Incident Management System (NIMS) in response to Homeland Security Presidential Directive (HSPD) 5—“Management of Domestic Incidents.” HSPD-5 directed the Secretary of Homeland Security to:¹²⁶

- Develop and administer a NIMS, and
- Develop the National Response Framework.

According to the NIMS framework, mutual aid or assistance agreements encourage entities to plan ahead and put in place mechanisms to acquire emergency assistance during or after a disaster. Utilities can acquire that assistance in the form of personnel, equipment, material, and other services.¹²⁷ Utilities are very familiar with the necessity and usefulness of these agreements, which add a level of redundancy to their system. State and local entities are usually familiar with the idea of assistance agreements and can create policies in which to foster that cooperation.

For example, according to a utility representative in 2013, the New York State regulators ordered all New York utilities to coordinate material resources to help reduce shortages in stock during large restoration efforts. As part of this effort, these utilities also worked on a framework for lending compensation.¹²⁸ Other industry representatives acknowledge the reduction in costs

¹²⁶ FEMA, 2008, *IS-700.A—National Incident Management System (NIMS): An Introduction*.

¹²⁷ FEMA, 2008.

¹²⁸ Central Hudson Gas & Electric Corporation, 2016a.

provided by these agreements as well the quicker response times as clear benefits to these agreements.^{129,130} In addition to aid agreements among utilities, utilities and contractors can enter into agreements that send fully equipped crews (e.g., linemen, supervisors, vehicles, equipment, and lines/poles) to assist in utility recoveries to major disasters.¹³¹

A utility service provider discussed some challenges typically associated with disaster response and recovery based on experience providing that support. Some regions that are subject to frequent major disasters are familiar with the need to respond and recover after specific natural hazards (e.g., hurricanes, tornadoes, snowstorms). Mutual aid is only one piece of the puzzle; certain equipment can be problematic to replace, such as transmission towers and special transmission transformers, which have long lead times. Although agreements may be in place for “sharing” transformers, companies usually have special specifications for transformers (e.g., different requirements for voltage or capacity), so the likelihood of getting a perfect match is low. According to utility representatives, many vendors offer services and equipment used by the utility industry for resilience. However, because of the differences in system designs and the different types of storms common to geographic areas of the country, these services vary greatly.¹³²

Table 13 identifies the potential threats, hazards, and vulnerabilities that could be addressed by mutual aid programs.

Table 13 Mutual Aid Programs: Threats, Hazards, and Vulnerabilities Potentially Addressed

Threats, Hazards, and Vulnerabilities Addressed	
 Ice, snow, and extreme cold weather	 Thunderstorms, tornadoes, and hurricane-force winds
 Storm surges, flooding, and increased precipitation	 Increasing temperature and extreme hot weather
 Earthquakes	 Physical attacks
 Aging infrastructure	 Capacity constraints
 Workforce turnover and loss of institutional knowledge	 Dependencies and supply chain interruptions

¹²⁹ PSE&G Long Island, 2016a.

¹³⁰ Meade, 2015.

¹³¹ Ibid.

¹³² PSE&G Long Island, 2016a.

4.8 Succession Planning, Knowledge Transfer, and Workforce Development

Succession planning has become a critical challenge to the utility industry. The electric power industry relies on a highly skilled labor force, which it has been struggling to maintain in recent years. With aging and retirement, today's workforce is taking substantial intellectual capital with them when they retire, and the number of replacement workers is inadequate to fill the jobs left by retirees.¹³³ Employers realize there will likely be skills or knowledge gaps as the older generation of workers retires. In March 2014, the Society for Human Resource Management (SHRM) launched a 3-year study titled "The Aging Workforce—State of Older Workers in U.S. Organizations." In the project press release, Human Resource professionals noted the difficulty in hiring skilled workers and stated that the loss of the "Baby Boomer" workforce will continue to affect industries over the next 5 years.¹³⁴ The Electric Subsector may be more susceptible to knowledge loss because of the specialized nature of the industry.

In December 2013, PricewaterhouseCoopers (PwC)¹³⁵ released a report titled "Power and Utilities Changing Workforce: Keeping the Lights on." According to that report, with the revival of the U.S. economy, older, skilled workers are considering retirement. At the same time, an ever-widening gap in the younger workforce is affecting the utility industry. There has been a shift in how the workforce approaches employment. Formerly, older workers typically stayed with companies throughout their career, whereas the younger workforce is more likely to shift jobs multiple times during their careers.¹³⁶ Both this report and the survey results of the SHRM project highlight the need for planning to account for this gap as well as strategies with which to mitigate these gaps.¹³⁷ The PwC report states that:

*The tendency of veteran utilities workers to retain valuable institutional knowledge in their heads and to pass it on orally, rather than systematically documenting and updating it, has compounded the problem. When these workers leave, intellectual capital is often lost if a formal program to capture know-how is absent.*¹³⁸

A key action for utilities to mitigate this risk is to intentionally plan to capture the knowledge and transfer it to younger staff. The SHRM survey results indicate that the more popular and effective mitigation measures utilities can do include:

- Increased training and cross-training efforts;
- Development of succession plans;

¹³³ Moeller, P., 2013, "Challenges of an Aging American Workforce," Website log post, *U.S. News Money* (June 19).

¹³⁴ Society for Human Resource Management, 2014, *SHRM and SHRM Foundation Launch Aging Workforce Project* (Press Release).

¹³⁵ PwC is a consulting company that, in the United States, focuses on 16 key industries and provides services in human resources as part of its portfolio.

¹³⁶ PwC, 2013, *Power and Utilities Changing Workforce—Keeping the Lights on* (December).

¹³⁷ SHRM, 2015, *The Aging Workforce—Basic and Applied Skills*, Society for Human Resource Management, Washington, D.C.

¹³⁸ PwC, 2013.

- Development of processes to capture institutional memory/organizational knowledge;
- Increased recruiting (and retention) efforts;
- Creation of new roles within the organization, specifically to bridge a skills or knowledge gap;
- Flexible work arrangements to attract a broader range of applicants;
- Increased automated processes; and
- Increased use of electric line training schools to prepare students before they are hired.

An interesting (and troubling) result of the survey revealed that of the 1,731 companies that participated, 34 percent had taken no steps to mitigate against these losses.¹³⁹

In August 2006, the DOE published a report to Congress regarding the Energy Policy Act of 2005.¹⁴⁰ This report focused on monitoring the trends in the skilled workforce in the electric power industry. The report identified the shortage in skilled labor and the magnitude of this shortage. This report also identified the loss of line workers and electric power and transmission engineers as the most concerning for the industry.

The DOE reported that university programs focused on power engineering are essential to the skilled engineering workforce of the future. Yet, the restructuring of the electric utility industry, along with wider interest in newer electrical engineering fields (e.g., microelectronics, computers, and communications) resulted in diminished support for power engineering programs, including a more recent decline in power engineering faculty, which further intensifies the problem.¹⁴¹

In the same report, the DOE noted that the electric industry is actively working to address the line worker shortage. Their strategies include building awareness, encouraging training initiatives, and increasing interest in the line worker profession at an early age.¹⁴² However, the path to a skilled, properly trained, and qualified line worker is a long one. Discussions with Meade representatives also brought up this barrier and a sobering point was raised.

“...[A]n electric system candidate must be trained, experienced and safe. If a mistake is made the person may electrocute or severely burn themselves or others, or compromise the electric system itself. Companies have training schools where a candidate starts out as an apprentice and then graduates to journeyman class over a period of up to 4+ years. The apprenticeship is a combination of classroom training and field experience with journeyman lineman on a crew. This is a profession where they [sic] are frequently no second chances. ...once you graduate you ... are placed with more experienced personnel. The problems you face are not all cookie cutter problems, [and placing] inexperienced personnel on problems caus[es] safety and liability concerns.”¹⁴³

¹³⁹ SHRM, 2015.

¹⁴⁰ DOE, 2006, *Workforce Trends in the Electric Utility Industry*, A Report to the United States Congress Pursuant to Section 1101 of the Energy Policy Act of 2005 (August).

¹⁴¹ Ibid.

¹⁴² Ibid.

¹⁴³ Meade, 2015.

Table 14 identifies the potential threats, hazards, and vulnerabilities that could be addressed by succession training, knowledge transfer, and workforce development measures.

Table 14 Succession Training, Knowledge Transfer, and Workforce Development: Threats, Hazards, and Vulnerabilities Potentially Addressed

Threats, Hazards, and Vulnerabilities (primary in black font; secondary in gray italics)	
 Physical attacks	 Cyber attacks
 Geomagnetic and electromagnetic pulses	 Capacity constraints
 Workforce turnover and loss of institutional knowledge	 Human error
 Dependencies and supply chain interruptions	 <i>Ice, snow, and extreme cold weather</i>
 <i>Thunderstorms, tornadoes, and hurricane-force winds</i>	 <i>Storm surges, flooding, and increased precipitation</i>
 <i>Increasing temperature and extreme hot weather</i>	 Earthquakes
 <i>Aging infrastructure</i>	

4.9 Business Continuity and Emergency Action Planning

A commonly agreed upon component of resilience is planning for business continuity during and after a disruption. In the International Standards Organizations (ISO) 22301, business continuity is defined as “the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.”¹⁴⁴ In FEMA’s NIMS framework, planning is a key component of preparedness activities in which utilities should participate. ISO 22301 standard includes suggested components of business continuity plans and other actions related to planning (i.e., employee awareness and training).

The availability of energy products, especially electricity, during emergencies, helps with response operations and helps return communities to normal operations. Recent, high-impact events, such as Superstorm Sandy, have demonstrated that the federal role in response, recovery and energy assurance planning has expanded. Federal, state, and local governments should work with the private sector for effective energy assurance planning.¹⁴⁵ Essential IT systems that are

¹⁴⁴ International Standards Organization, 2012, *ISO 22301: Societal Security—Business Continuity Management Systems—Requirements* (May).

¹⁴⁵ DOE OE-NASEO, 2012, *2012 National Energy Assurance Planning Conference: After Action Report*, June 28–29, Gaylord Hotel and Convention Center, National Harbor, Maryland.

vital for response and recovery efforts, such as outages systems, need to be identified as critical systems and should have built-in redundancies, which act to reduce the likelihood of failure and/or increase the ability to recover quickly if failure occurs.

Common items utilities can consider in a business continuity management plan, in addition to the construction of the plan, are the awareness and training activities for employees as well as tabletop exercises and simulations, where personnel are trained to respond effectively. Utilities should also keep plans current by incorporating routine updates derived from lessons learned from exercises and real-world scenarios.¹⁴⁶ The sections below highlight different components of business continuity planning, including communications, exercises, and information sharing and lessons learned.

Table 15 identifies the potential threats, hazards, and vulnerabilities that could be addressed by business continuity and emergency action planning measures.

Table 15 Potential Business Continuity and Emergency Action Planning: Threats, Hazards, and Vulnerabilities Potentially Addressed

Threats, Hazards, and Vulnerabilities	
 Ice, snow, and extreme cold weather	 Thunderstorms, tornadoes, and hurricane-force winds
 Storm surges, flooding, and increased precipitation	 Increasing temperature and extreme hot weather
 Earthquakes	 Physical attacks
 Cyber attacks	 Geomagnetic and electromagnetic pulses
 Human error	 Dependencies and supply chain interruptions

4.9.1 Customer Communication

The utilities depend on communications during and after an event, not only as a mechanism to assess damaged equipment but also to relay outage information and restoration times to its customers. Utilities use their Websites to communicate with customers by providing preparation checklists, outage maps, options to report/check status of outage, special needs requests, and safety information.^{147,148}

Representatives from one utility noted that when responding to a storm or a major outage event, communication with customers and other stakeholders is nearly as important as the actual restoration of service. As a result, they have established several initiatives over the last 5 years to

¹⁴⁶ DOE OE, 2010.

¹⁴⁷ Con Edison, 2016a.

¹⁴⁸ PSE&G Long Island, 2016a.

improve communications to their customers through their Websites, mobile applications, automated texting, social media, as well as improved coordination with traditional communication outlets (press releases and direct phone communication). To further increase situational awareness, utilities have started to establish a direct link between the computers that are used in the field by the line forces and the outage information that is available directly to the customers. The linemen can enter an estimated time of restoration, and it will be published on the external facing Website with no human intervention.¹⁴⁹

4.9.2 Information Sharing

Several industry- and government-level councils serve as information gathering and sharing entities to the Electric Subsector. The National Infrastructure Protection Plan, published in 2003, established two coordinating councils, one private sector and one government to establish a government-private sector partnership model. These two councils are described below¹⁵⁰:

- The Electricity Subsector Coordinating Council (ESCC), initially established in 2004, was organized and administered by companies in the electric power industry to meet regularly to coordinate policy-related activities designed to “improve the reliability and resilience of the electricity subsector, including physical and cyber infrastructure.”
- The Energy Sector Government Coordinating Council (EGCC), also established in 2004, is the government counterpart to the ESCC. The EGCC is chaired by the DOE and DHS, incorporating other agencies at all levels of government with interest in energy security. The EGCC plays a key role in implementing DOE’s Energy Sector-Specific Plan,¹⁵¹ collaborating with the ESCC to develop and prioritize security programs and initiatives.

Other organizations have been established that focus specifically on grid security, but also serve as an information sharing mechanism for industry.¹⁵² They are listed below:

- The ES-ISAC, established in 1998, is the electric power industry’s primary communications channel for security-related information, situational awareness, incident management, and coordination. It serves as the federal entity for collecting and distributing information within the sector. Operated by NERC in collaboration with the DOE and ESCC, the center’s members may anonymously share security-related incident information with the ES-ISAC by means of a secure Internet portal. Registered users receive information on security threats and alerts, remediation, task forces, events, and other security-specific resources. It is important that these approaches complement and properly interface with the National Response Framework and state energy assurance plans.

¹⁴⁹ Central Hudson Gas & Electric Corporation, 2016a.

¹⁵⁰ Parfomak, P.W., 2014, *Physical Security of the U.S. Power Grid: High Voltage Transformer Substations*, Congressional Research Service Report.

¹⁵¹ *National Infrastructure Protection Plan (NIPP) Energy Sector-Specific Plan*, 2015.

¹⁵² Ibid.

- NERC’s Critical Infrastructure Protection Committee (CIPC) coordinates organizations’ security initiatives and advises its Board of Trustees, its standing physical and cybersecurity committees, and the ES-ISAC. One of the CIPC’s key functions is developing, reviewing, and revising security guidelines, as well as assisting in the development and implementation of NERC standards.

4.9.3 Exercises

Training and exercising are critical components of resilience. In FEMA’s NIMS framework, effective emergency management and incident response begin with several preparedness activities to include training and exercising. Creating forums to bring stakeholders together for a dialogue around issues, even via a tabletop exercise, can be catalysts for making things happen. Oftentimes, these discussions can lead to “aha” moments or finding solutions “outside the box.”¹⁵³

As one example, NERC’s GridEx exercises are sector-wide security exercises designed “to execute the electricity sector’s crisis response to simulated coordinated cybersecurity and physical security threats and incidents, to strengthen utilities’ crisis response functions, and to provide input for lessons learned.”¹⁵⁴ To date, three GridEx’s have been conducted: GridEx (November 16–17, 2011); GridEx II (November 13–14, 2013); and GridEx III (November 18–19, 2015).¹⁵⁵

Regardless at which level (i.e., national, regional, local community) an exercise is held, the information exchanged and interactions among different stakeholders are invaluable. The National Association of State Energy Organizations (NASEO) regional exercises held as part of the state energy assurance planning effort are set up to bring in multiple interdependencies. An exercise is a great avenue for getting people to think about things they have not considered before.¹⁵⁶

4.10 Models

Models meant to predict responses of the grid to disruption or predict outages due to a disruption are highly desired in the electric power industry. These models have primarily focused on natural hazards to inform utility risk analysis. As the importance of the nexus between electricity and telecommunications has grown apparent, however, models focusing on the impacts of cyber defenses are also in high demand. In addition, utilities are using modeling to prepare integrated resource plans, which allow a utility to plan for meeting forecasted annual peak and energy demand. Though models can be useful tools for informing decisions, they do have limitations.

¹⁵³ Pillon, 2015.

¹⁵⁴ NERC, 2013, *GridEx*, Website.

¹⁵⁵ The after-action summary report for GridEx III has yet to be released.

¹⁵⁶ Pillon, 2015.

No model will ever provide an absolute answer with certainty. Typical models have one or more assumptions associated with their construction. It is critical to keep these assumptions in mind when interpreting the results. Models are not meant to provide *the* answer or solution that *must* be correct. They are only meant to provide general guidance to help decisionmakers make informed decisions.

Data are key for developing adequate models. Predictive models for weather often use historic occurrences for planning, building, protecting, and retrofitting of existing infrastructure. Utilities have been using these types of models for several years. Because of the time and expense associated with building new infrastructure or retrofitting existing infrastructure, plans and designs are often based on worst-case scenarios.^{157,158,159}

One utility contacted as part of this effort provided an example of a modeling prioritization. This northeast utility, in conjunction with stakeholder collaboration, developed a risk assessment and prioritization model to gauge, in terms of risk reduction to customers and critical infrastructure, both the collective impact of the utility's programs and their relative merits across different components of the company's system. The output of the model quantifies and ranks the reduction in risk associated with each of the storm-hardening projects related to the company's transmission, substation, underground network, and overhead distribution systems.¹⁶⁰

The model establishes the value of each of the utility's storm-hardening initiatives in terms of the magnitude of the reduction in risk at each targeted asset. This metric helps to demonstrate a cost causality linkage between capital funding allocated for storm hardening and the reduction in risk obtained via that investment. The output of the model, however, is not intended to be a stand-alone litmus test of each project's value. The company applies engineering judgment reflecting system design and operating characteristics and experience in the selection of eliminated programs while considering the prioritization ranking. Key components of the model are¹⁶¹:

- Location-specific information regarding high-rise residential buildings and municipal critical infrastructure (e.g., hospitals and water treatment facilities);
- Location-based flood probabilities provided through proprietary New York City inundation models;
- Wind damage probabilities derived from historic wind gust frequency distributions;
- Costs to storm harden the utility's facilities; and
- Projected outage durations in absence of and after implementation of effective storm mitigation.

¹⁵⁷ Con Edison, 2016a.

¹⁵⁸ Central Hudson Gas & Electric Corporation, 2016a.

¹⁵⁹ PSE&G Long Island, 2016a.

¹⁶⁰ Con Edison, 2016a.

¹⁶¹ Ibid.

Table 16 identifies the potential threats, hazards, and vulnerabilities that could be addressed by models.

Table 16 Models: Threats, Hazards, and Vulnerabilities Potentially Addressed

Threats, Hazards, and Vulnerabilities	
 Ice, snow, and extreme cold weather	 Thunderstorms, tornadoes, and hurricane-force winds
 Storm surges, flooding, and increased precipitation	 Increasing temperature and extreme hot weather
 Earthquakes	 Physical attacks
 Cyber attacks	 Geomagnetic and electromagnetic pulses
 Aging infrastructure	 Capacity constraints
 Dependencies and supply chain interruptions	

This page intentionally left blank

5 Challenges and Gaps in Addressing Resilience

As described in the previous section, there are a myriad of resilience options that utilities can implement. However, efforts to enhance resilience can often be challenging for utilities. Resilience investments can be expensive and require significant capital and time to implement. This necessitates the need for utilities to prepare a rate case that includes sufficient justification, which can be a challenge when investments involve preparation and planning for events that have not yet happened. In addition, gaps inhibit resilience enhancement measures, including uncertainties in global climate change, development and changes in state and local policies and regulations regarding energy infrastructure resilience, and the incomplete understanding of the interactions between energy infrastructure and other systems of critical infrastructure. This section expands upon these challenges and gaps. The information presented herein is the result of discussions with SMEs and industry partners, as well as open-source research.

Table 17 illustrates some common resilience enhancements, with examples, as identified by utilities and research.

Table 17 Electric Utility Resilience Enhancement Options

Resilience Enhancement Options	Definition	Example
Hardening	Physical changes that improve the durability and stability of specific pieces of infrastructure	Raising and sealing water-sensitive equipment
Security measures	Measures that detect and deter intrusions, attacks, and/or the effects of manmade disasters	In-depth security checks on all employees, badged entry and limited access areas, and surveillance and monitoring
Maintenance and general readiness	Routine efforts to minimize or prevent outages	Vegetation management and regular inspection and replacement of worn-out components
Modernization, control enhancements, and smart-grid technology	Technology and materials enhancements to create a more flexible and efficient grid	Integration of smart-grid technologies, such as smart meters and phasor measurement units
Diversified and integrated grid	Transitioning of the grid from a centralized system to a decentralized generation and distribution system	Integration of distributed generation sources, such as renewable energy sources and establishment of microgrids
Redundancy, backup equipment, and inventory management	Measures to prepare for potential disruptions to service	Maintenance of spare equipment inventory, priority agreements with suppliers, and maintenance of a supply of backup generators
Mutual aid programs	Agreements that encourage entities to plan ahead and put in place mechanisms to acquire emergency assistance during or after a disaster	Agreements between utilities to send aid or support after a disaster

Table 17 (Cont.)

Resilience Enhancement Options	Definition	Example
Succession training, knowledge transfer, and workforce development	Planning for transfer of knowledge and skills from a large retiring workforce, to a smaller, younger workforce	Proactive efforts to create training and cross-training programs and succession plans
Business continuity and emergency action planning	A formal plan that addresses actions and procedures to maintain operations preceding an event	Components can include employee awareness, training, and exercising
Models	Mathematical constructs that provide information on performance and/or disruptions to aide in decisionmaking	Probabilistic risk models to assist in predicting outage impacts after an event

5.1 Predictability of Storms and System Responses to Climate Change

The development of predictive models has always been of interest to the electric power industry. The development of adequate models allows utilities to understand potential consequences of an event and plan for mitigating those consequences before an event happens. Through an interview, a utility representative remarked that “predictive model[ing] remains a significant interest in the industry, both in the short term so that a utility can request the correct resources for a specific event and in the long term, so the utility can determine the areas that are at the greatest risk of failure and then make the best investments in infrastructure improvement.”¹⁶² The output of any predictive model will contain some amount of error. Historically, past events (i.e., natural hazards) have been used to help formulate parameters of the model in an attempt to minimize error. However, uncertainty is now multiplied as the range and extremes of weather phenomena (i.e., because of climate change) are moving into unmapped territory. The climatic changes forecasted to manifest over the next 50–100 years should also impact upgrades to existing and development of new technologies and infrastructure. The uncertainties associated with the accepted climate change models, in addition to human behavioral responses to those climate changes (i.e., shifting of population centers), exacerbate the ability to plan for future infrastructure needs.

5.2 Cost Recovery and Stranded Investments

Electric energy infrastructure owners consist of federal agencies, municipal governments, rural cooperatives and investor-owned utilities (an overwhelming majority). In addition to the different types of ownership, due to deregulation, customers can receive power from separate generation, transmission, and distribution companies. Those complexities are further

¹⁶² Central Hudson Gas & Electric Corporation, 2016a.

compounded by the rates that local utilities charge, which are generally regulated by state agencies.¹⁶³

In the midst of these complexities, electric power customers expect power to be delivered consistently with minimal disruptions. Keeping the lights on is an equally important imperative to the utilities, as disruptions can result in a significant loss of revenue. Satisfying customer expectations and minimizing revenue loss are sufficient motivators for power companies to invest in processes and solutions that minimize downtime, both on blue sky days and on days when an adverse event shuts down the power.¹⁶⁴

Federal and state regulators have jurisdiction over the bulk power system, while state or local regulations typically drive local distribution rates.¹⁶⁵ This regulatory model can lead to tensions between the regulators and industry to implement resilience-enhancing options. The utilities must build rate cases to justify the installations of any new measures and/or cover the cost of current costs of operation, which may have changed. Part of this rate case is providing justification that these costs are reasonable and prudent and can include showing estimates for return on investment (ROI). Interestingly, in the case of cybersecurity enhancements, the perceived risk of a cyber attack has been sufficient to gain commission support for utility rate cases requesting recovery for cybersecurity measures, even though these investments have not yet been shown as reasonable and prudent. For resilience measures, it can be difficult to calculate an ROI, given that their benefit typically is only fully realized upon the advent of a major event. This may be difficult to justify in front of a public utility commission and the end use customers. Utilities are sensitive to balancing the need to enhance resilience and the costs associated with enhancing that infrastructure to include burdening their customers with increased rates.^{166,167} Some important trade-offs should be considered, however. Utilities and regulators should consider compromises that balance affordable and stable rates for customers and the need to invest in upgraded and new infrastructure for tomorrow. Investing in resilience is like buying insurance for future disasters or changes. Small “premium” payments on changes now could result in far less expense to recover after a disaster as well as a smaller impact during the event.¹⁶⁸ Given these sensitivities, rate-based recovery continues to be the most common method to support long-term investment and damage repairs after major events.¹⁶⁹ Utility commissions tend to be more willing to allow utilities recover the cost for resilience investments following a major event or disaster (e.g., Superstorm Sandy or the 2003 Northeast Blackout).

¹⁶³ ASCE, 2013.

¹⁶⁴ Barrett et al., 2013.

¹⁶⁵ ASCE, 2013.

¹⁶⁶ Con Edison, 2016a.

¹⁶⁷ Central Hudson Gas & Electric Corporation, 2016a.

¹⁶⁸ Barrett et al., 2013.

¹⁶⁹ DOE EPSA, 2015.

The Edison Electric Institute’s (EEI’s) comments on the Quadrennial Energy Review (QER)¹⁷⁰ recommended that the industry be allowed to develop “innovative alternative utility rate design models.” The increased prevalence of distributed generation (e.g., microgrids, solar, wind, and smart vehicles) and the challenges with incorporating those typically intermittent power resources into the grid almost necessitate a new model. New design models will allow costs to be allocated to the proper customers while maintaining the need to keep the grid reliable and resilient. The EEI also suggested developing additional federal programs or tax provisions designed to generate consistent funding to implement changes before and after extreme events. These types of programs will allow federal assistance in preparing for the changing environment for energy infrastructure and promote proactive investments in resilience-enhancing activities.

5.3 Communication and Workforce

The continuum of resilience-related activities spans from complicated to simplistic, expensive to inexpensive, and time-consuming to instantaneous in implementation. Many discussions involving resilience of the electric grid center on changes to the actual infrastructure, for example, upgrading existing infrastructures or installing new components. In fact, utility management, employees, and state and local entities can employ various measures (that are neither costly nor time-consuming) to enhance resilience. Several references (i.e., ISO 22301,¹⁷¹ British Standard 25999-2,¹⁷² and American National Standards Institute/American Society for Industrial Security SPC.1¹⁷³) focus on the creation of robust plans, including business continuity, emergency preparedness, or disaster response plans. Some components are common to all plans, regardless of the type. Examples include establishing key points of contact; coordinating interactions with outside responders; and training, exercising, and regularly maintaining the plan.¹⁷⁴

In June 2012, the DOE OE-NASEO held a joint planning meeting titled “2012 National Energy Assurance Planning Conference.” This conference was the culmination of 3 years of effort associated with the DOE’s American Recovery and Reinvestment Act of 2009 State and Local Energy Assurance Program (SLEAP).¹⁷⁵ The DOE OE-NASEO conference aimed to collect lessons learned and experiences from state and local energy assurance planners. Notable recurring themes collected in this after-action report and proposed solutions included¹⁷⁶ the following points:

¹⁷⁰ EEI, 2014, *Infrastructure Resilience and Vulnerabilities – Cyber, Physical, Climate, Interdependencies: Comments of the Edison Electric Institute*, Quadrennial Energy Review, Department of Energy (June).

¹⁷¹ International Standards Organization, 2012.

¹⁷² British Standards Institute, 2006, *BS 25999-1: Business Continuity Management—Part 1: Code of Practice* (November).

¹⁷³ ASIS International, 2009, *ASIS SPC.1-2009: Organizational Resilience: Security, Preparedness, and Continuity Management Systems—Requirements with Guidance for Use* (March).

¹⁷⁴ ISO 22301 has become the industry standard for business continuity management since May 2012.

¹⁷⁵ DOE OE-NASEO, 2012, *2012 National Energy Assurance Planning Conference: After Action Report*.

¹⁷⁶ Ibid.

- **Communications.** Know the key points of contact and establish relationships prior to emergencies. Have robust communication technologies and protocols in place. Develop plans for communicating with the public.
 - Involve community disaster responders (i.e., law enforcement, fire department, and healthcare) in the planning and exercising of response and continuity plans.
 - Coordinate with state and local partners who are not directly involved in emergency response. Focus on state officials incorporating the energy assurance plan (EAP) into the state emergency operations plan to raise the importance of energy assurance policies and procedures with partners.
- **Roles and responsibilities.** Clearly define in plans any roles and responsibilities.
 - Review contracts and authorities during energy assurance planning to ensure that they work as expected in an emergency.

These are a few of many lessons learned reported during that conference. Multiple panel discussions looked at aspects of energy planning and execution, including successful approaches to state and local energy assurance planning, private sector energy assurance initiatives, interdependencies, energy emergency preparedness, and plans to action to build energy resilience. Another recurring theme at the conference centered on coordination and collaboration among state and local governments, utilities, and other critical infrastructure.

5.4 Coordination and Collaboration

Maintaining electric power during and post emergency touches almost every component of a community. A community's dependence on electric power necessitates collaboration among a disparate set of entities, including state and local governments, utility providers, and owners of other critical infrastructure. The dependence on electric infrastructure for operations should require a shared responsibility among the entities for keeping it operational; doing so will increase resilience across the entire community.¹⁷⁷

Enhancing coordination and collaboration among these entities depends on: (1) awareness of connections and impacts of these connections and (2) information available and the ability to share that information. Exchanging information that could be considered business sensitive has always been problematic, even during an emergency or in the recovery phase. Conversations with industry revealed that data protection issues hamper governmental and commission approval of projects because of the large amounts of secure information needed to inform these decisions.¹⁷⁸

¹⁷⁷ Barrett et al., 2013.

¹⁷⁸ Meade, 2015.

To increase the ability to share infrastructure—and threat—information, new and/or improved opportunities need to be explored and developed. According to the EEI responses to the QER, solutions to any barriers to information sharing “should seek to reduce liabilities associated with information sharing.”¹⁷⁹ The main themes identified in the DOE OE-NASEO After Action Report included communications, shared responsibilities, and the importance of recognizing interdependencies and the impacts of disruptions to these interdependencies. These lessons learned were the result of the exercises conducted through the 3-year period that the SLEAP was in effect. Some notable takeaways from the after-action report are provided below:

- The interface between government and industry is critical. Government depends on industry for data to perform situational assessments, and industry depends on government to provide the status of the sector at large. It is essential to build relationships and develop processes and procedures for sharing information that is critical to getting the data needed to perform a situational assessment.
- State and local governments need to understand energy industry interdependencies with other sectors and prepare for them. Doing so will improve recovery time and help avoid unintended consequences.

Suggestions involving coordination and information sharing from the DOE OE-NASEO report include the following: collecting and updating a state’s energy profile to understand the current generation, transmission, and distribution infrastructure; outlining and understanding critical interdependencies between the electric infrastructure and other critical infrastructure prior planning; and developing a common platform that enhances a common operating picture for government, utilities, and owners of other critical infrastructure during and after an event.¹⁸⁰

In February 2015, the Secretary of Energy signed a memorandum of understanding with NASEO, the National Association of Regulatory Utility Commissioners (NARUC), the National Governors Association, and the National Emergency Management Association.¹⁸¹ It provided points of contact in each state and serves as a means to share, and exchange, information on planning for, and responding to, energy emergencies. It also supported a secure cooperative communications environment for state and local government personnel with access to information on energy supply, demand, pricing, and infrastructure.

Finally, the education of the consumer population, specifically the individual residential consumers, is important in communication and collaboration. Resilience efforts can cost a significant amount of money, and the utilities will seek to recover these costs, typically via the customers. The customers, especially individual residential customers, however, have a difficult time understanding improvements that are not immediately or only incrementally felt. Situational

¹⁷⁹ EEI, 2014.

¹⁸⁰ DOE OE-NASEO, 2012.

¹⁸¹ DOE OE-NASEO, 2015, *Terms of Reference to the Agreement on Federal and State Energy Emergency Coordination, Communications, and Information Sharing*, in agreement with the National Association of Regulatory Utility Commissioners, the National Governor’s Association, and the National Emergency Management Association (June 24).

awareness and education are as important at the individual end user level as they are for state, local, and private sector critical infrastructure owners and operators.¹⁸²

The following summarizes need for enhanced communication, collaboration, and understanding for all entities involved in understanding the risk to a community, the importance of energy infrastructure in that risk picture, and the preparation for disruptions to the system:

As a nation, we will need to find better ways to manage these areas of shared responsibility stemming from current and future evolutions of the aggregate and shared risk picture. This requires finding solutions that blend broader risk management needs for a more resilient electrical grid with the private sector's ability to invest in ways that meet challenges effectively and efficiently. It also requires an open dialogue about the full costs and potential benefits of a more interactive and modernized smart grid that allows consumers to help by reducing demand during peak periods and provides deeper insights into the otherwise opaque real-world operating conditions of the grid itself.¹⁸³

5.5 Governance Gaps

Infrastructure resilience is a whole community issue. As such, the utilities and the private sector can work toward resilience in complementary ways. For example, the utilities can work on the process, procedures, and construction, while the private sector can prepare for the loss of electricity during a disaster and assist in community preparation in resilience. Although utilities are making investments to increase resilience, long-term solutions rely on the identification and management of shared risks and identification of governance gaps. Governance gaps in this context are defined as areas of shared risk where there is no clear identification or responsibility assigned to one or more entity. This lack of clarity can lead to an increase in consequences or impacts of an event because these areas are often overlooked.¹⁸⁴

One common governance gap is realized during low-probability, high-consequence events, such as Superstorm Sandy. The magnitude of the disruptions caused by this type of event highlights, even further, the need for coordinated efforts among state, local, and private sector entities. However, the identification of the shared risks and assignment of who is responsible for what is often not considered or is considered but never discussed in detail. Lessons on the importance of the identification of the shared risks and the identification of the entities responsible to address those risks often occur after a major event. Multi-entity exercises can help shed light on these governance gaps and assist in preparing for these disastrous events before they happen. The results of the regional exercises held as part of the SLEAP efforts identified the need for multi-organizational coordination. Several panel discussions in the June 2012 meeting focused on sustaining energy emergency preparedness, infrastructure interdependencies and building community resilience, and moving plans to actions that build energy resilience.¹⁸⁵

¹⁸² Barrett et al., 2013.

¹⁸³ Ibid.

¹⁸⁴ Ibid.

¹⁸⁵ DOE OE-NASEO, 2012.

As previously mentioned, due to deregulation, separate entities—often private companies—can operate the electric power grid (illustrated in Figure 1). While consumers often absorb the recovery costs associated with resilience improvements, private investment in electricity infrastructure is an important component to consider from a governance perspective. Governance actions, such as public policies, regulations, and processes, play a role in the nature and magnitude of private investment in electricity infrastructure.¹⁸⁶ Policies and legislation implemented through state and local governments, developed in concert with other members of the community as well as the utilities, can help secure funds as well as remove barriers to implementing resilience measures.

5.6 Future Threats and Hazards

While utilities, state and local governments, and other private sector entities struggle to make improvements to address the existing landscape of threats and hazards, they also face another significant gap—addressing future risks that may not be in the typical time frame for planning or amenable to traditional methods of planning. Utilities typically base their planning assumptions on historic data; however, the effects of climate change can lead to ever-changing surroundings and uncertainty in the future. Global climate has already started to deviate from historic averages. According to the Intergovernmental Panel on Climate Change (IPCC) Special Report,¹⁸⁷ in the haste to rebuild infrastructure as quickly as possible after a disaster, utilities could miss an opportunity to improve their infrastructure rather than rebuild it to the previous standard. With the advent of deviations in those patterns due to climate change, historic trends could be misleading, as frequency, magnitude, or new events manifest themselves over the next half century, thus leading to infrastructure that is unable to perform as efficiently or at all. Utilities should focus their efforts on climate change adaptation strategies that can reduce exposure and vulnerability to extreme weather and climate events, thus reducing disaster potential, as well as increasing resilience to the risks that cannot be eliminated.¹⁸⁸

In addition to the uncertain and shifting landscape of natural disasters, other occurrences of manmade threats are increasingly ambiguous due to the unpredictability of terrorist actions, the prediction of and protection against cyber attacks, as well as more traditional manmade threats (e.g., worker errors or insider threats using knowledge of the system). Another type of risk is the interdependency among the electric grid and other systems of critical infrastructure, especially telecommunications. As with electricity, telecommunications (phones as well as Internet) are critical to the operations of modern times. Most, if not all, critical infrastructure relies on telecommunications in some way. Electric power requires telecommunications to maintain information and responsiveness across the grid, especially as the grid starts to get “smarter.”¹⁸⁹ Supervisory control and data acquisition (SCADA) systems are a common telecommunications component of greatest importance to the operations of the grid. This risk can build upon itself,

¹⁸⁶ ASCE, 2013.

¹⁸⁷ IPCC, 2012, *Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation*, Special Report of Working Groups I and II of the IPCC.

¹⁸⁸ Barrett et al., 2013.

¹⁸⁹ Ibid.

leading to increasing consequences that depend on how interconnected the systems are and how quickly the system can recover. For example, a disruption in the grid can impact telecommunications systems that support the function and operation of other portions of the grid, which can in turn cause further disruptions in the grid and generate cascading failures.

The items discussed in this section touch on a subset of the landscape of future risks for electric power. The 2013 ASCE Failure to Act report identified several risks, including uncertainty about supply and demand, impacts of distributed generation, future prices of fossil fuels, incorporation of smart grids and microgrids, regulations controlling greenhouse gas emissions and rate of adoption of more renewable power options, and the complexity of integrating those variable power sources into the grid. These types of uncertainties can all make it more difficult to forecast future performance, cost, and ROIs.¹⁹⁰

¹⁹⁰ ASCE, 2013.

This page intentionally left blank

6 Conclusions

The importance of the electric grid in our society and the resilience of the grid to disruption have come to the forefront of our attention. This report provides insight into resilience from the perspective of the electric utilities. The electric power industry is vulnerable to a wide range of threats, hazards, and vulnerabilities. Utility representatives and open-source research, however, revealed some of the most common resilience enhancement options available for and applied by electric utilities. Although much has been done to address resilience of this sector's multi-hazard environment, challenges and gaps remain. Some of the primary issues are outlined below:

- Resilience investments can primarily be anticipatory in nature, requiring significant capital and time to implement. Rate cases that include sufficient justification can be a challenge when investments involve preparation and planning for events that have not yet happened.
- ROI on resilience options can be difficult to quantify, given that their benefit typically is only fully realized upon the advent of a major event.
- Predictive models for future climate impacts on the electric utility contain large amounts of uncertainty. Utilities need to plan for an uncertain future that lies outside the historic range of planning factors.
- The dependence of other critical infrastructure assets and system upon the Electric Subsector further escalate societal consequences upon the loss of electric power.

Continued research and development to identify new technologies, legislative and grid architectural changes, and new market cost models are all part of the future of grid resilience. It will take researchers, utilities, academia, and government at all levels to move resilience of the electric power industry forward.

This page intentionally left blank

7 Works Cited

ABB, 2015, *Why Use Reclosers?* Available at <http://www.abb.com/product/ap/db0003db004279/b0b2c0094a20cb88c1257a0e004c685a.aspx>.

Alliance to Save Energy, 2012, *CHP Kept Schools, Hospitals Running Amid Hurricane Sandy* (December). Available at <http://www.ase.org/resources/chp-kept-schools-hospitals-running-amid-hurricane-sandy>.

Amortex, 2015, *Fire Containment & Ballistic Protection for Critical Infrastructure from Amortex*. Available at <http://www.aecinfo.com/fire-containment-ballistic-protection-for-critical-infrastructure-from-armortex-86520/news.html>.

Apt, J., L.B. Lave, S. Talukdar, M.G. Morgan, and M. Ilic, 2004, “Electrical Blackouts: A Systemic Problem,” *Issues in Science and Technology* 20(4): 55–61 (Summer).

ASCE (American Society of Civil Engineers), 2013, *Failure to Act: The Economic Impact of Current Investment Trends in Electricity Infrastructure*, prepared by Economic Development Research Group, Inc. Available at http://www.asce.org/uploadedFiles/Issues_and_Advocacy/Our_Initiatives/Infrastructure/Content_Pieces/failure-to-act-electricity-report.pdf.

ASIS (American Society for Industrial Security) International, 2009, *ASIS SPC.1-2009: Organizational Resilience: Security, Preparedness, and Continuity Management Systems—Requirements with Guidance for Use* (March). Available at https://www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf.

Barrett, J.M., J. Harner, and J. Thorne, 2013, *Ensuring the Resilience of the U.S. Electrical Grid*, Lexington Institute (January).

Barringer, F., 2015, “Troubling Interdependency of Water and Power,” *The New York Times*, Energy & Environment (April 22).

Bipartisan Policy Center, 2014, *Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat*, a Report from the Co-chairs of the Bipartisan Policy Center’s Electric Grid Cybersecurity Initiative (February).

British Standards Institute, 2006, *BS 25999-1: Business Continuity Management—Part 1: Code of Practice* (November). Available at https://www.pea.co.th/BCM/DocLib/BS_25999-1.pdf.

Central Hudson Gas & Electric Corporation, 2016a, Personal Communication.

Central Hudson Gas & Electric Corporation, 2016b, *About Us: Our Mission Statement*, Website. Available at http://www.centralhudson.com/about_us/index.aspx.

Central Hudson Gas & Electric Corporation, 2016c, *Projects*, Website. Available at <http://www.centralhudson.com/projects/index.aspx>.

Chertoff Group, the, 2014, *Addressing Dynamic Threats to the Electric Power Grid through Resilience*, Washington D.C. (November).

Con Edison, 2016a, Personal Communication.

Con Edison, 2016b, *About Us*, Website. Available at <http://www.coned.com/aboutus/>.

Con Edison, 2016c, *Facts and Background*, Website. Available at https://www.coned.com/newsroom/information_facts.asp.

Con Edison, 2016d, *Con Edison Wins 2015 ReliabilityOne™ Award for Outstanding System-Wide Reliability*. Available at <https://www.coned.com/newsroom/news/pr20151023.asp>.

Consumers Energy, 2014, *Consumers Energy Company's Report in Response to MPSC Order in Case No. U-17542* (February 7).

DOE (U.S. Department of Energy), 2006, *Workforce Trends in the Electric Utility Industry*, a Report to the United States Congress Pursuant to Section 1101 of the Energy Policy Act of 2005 (August).

DOE, 2008, *The Smart Grid: An Introduction*. Available at <http://energy.gov/oe/technology-development/smart-grid/smart-grid-primer-smart-grid-books>.

DOE, 2013, *U.S. Energy Sector Vulnerabilities to Climate Change and Extreme Weather*, DOE/PI-0013 (July).

DOE, 2016, *DOE Grid Modernization Laboratory Consortium (GMLC) – Awards*. Available at <http://energy.gov/doe-grid-modernization-laboratory-consortium-gmlc-awards>.

DOE EPSA (Energy Policy and Strategic Analysis), 2015, *Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure* (April).

DOE EPSA, 2016, *About the Quadrennial Energy Review*, Website. Available at <http://energy.gov/epsa/quadrennial-energy-review-qer>.

DOE OE (Office of Electricity Delivery and Energy Reliability), 2010, *Hardening and Resiliency U.S. Energy Industry Response to Recent Hurricane Seasons* (August).

DOE OE, 2012, *American Recovery and Reinvestment Act Energy Assurance Planning Bulletin*, Vol. 4, No. 4.

DOE OE, 2015b, *About Us*, Website. Available at <http://energy.gov/oe/about-us>.

DOE OE, 2015c, *State and Regional Energy Risk Assessment Initiative—State Energy Risk Profiles*, Website. Available at <http://energy.gov/oe/state-energy-risk-assessment-initiative-state-energy-risk-profiles>.

DOE OE, 2015d, *State and Local Energy Assurance Planning*, Website. Available at <http://energy.gov/oe/services/energy-assurance/emergency-preparedness/state-and-local-energy-assurance-planning>.

DOE OE-NASEO (Office of Electricity Delivery and Energy Reliability-National Association of State Energy Officials), 2012, *2012 National Energy Assurance Planning Conference: After Action Report*, June 28–29, Gaylord Hotel and Convention Center, National Harbor, Maryland. Available at <http://energy.gov/oe/downloads/2012-national-energy-assurance-planning-conference-after-action-report-august-2012>.

DOE OE-NASEO, 2015, *Terms of Reference to the Agreement on Federal and State Energy Emergency Coordination, Communications, and Information Sharing*, in agreement with the National Association of Regulatory Utility Commissioners, the National Governor’s Association, and the National Emergency Management Association (June 24). Available at [http://www.naseo.org/Data/Sites/1/documents/energyassurance/documents/final-eeac-agreement-\(february-2016\).pdf](http://www.naseo.org/Data/Sites/1/documents/energyassurance/documents/final-eeac-agreement-(february-2016).pdf).

DTE Electric Company, 2014, *DTE Electric Company’s Response to MPSC Order U-17542* (February 7).

EEI (Edison Electric Institute), 2016, Website. Available at <http://www.eei.org/Pages/default.aspx>.

EEI, 2014, *Infrastructure Resilience and Vulnerabilities – Cyber, Physical, Climate, Interdependencies: Comments of the Edison Electric Institute*, Quadrennial Energy Review, Department of Energy (June). Available at <http://energy.gov/sites/prod/files/2015/03/f20/Edison%20Electric%20Institute%20Comments%20and%20Resources-%20QER%20-%20Enhancing%20Infrastructure%20Resiliency%20FINAL.pdf>.

EIA (U.S. Energy Information Administration), 2015, *Annual Energy Outlook 2015: With Projections to 2040*, DOE/EIA-0383(2015), DOE Office of Integrated and International Energy Analysis (April).

Emprimus, 2015, *Effects of GMD & EMP on the State of Maine Power Grid*, prepared in partnership with Central Maine Power, Emera, Maine.

EPRI (Electric Power Research Institute), 2001, *The Cost of Power Disturbances to Industrial and Digital Economy Companies* (June).

EPRI, 2013, *Enhancing Distribution Resiliency—Opportunities for Applying Innovative Technologies* (January).

EPRI, 2014a, *The Integrated Grid: Realizing the Full Value of Central and Distributed Energy Resources*, Technical Results (February). Available at <http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002002733>.

EPRI, 2014b, *The Integrated Grid Phase II: Development of a Benefit-Cost Framework*, Technical Results (May). Available at <http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002004028>.

EPRI, 2016, *Our Members*, Website. Available at <http://www.epri.com/About-Us/Pages/Our-Members.aspx>.

Executive Office of the President, 2013, *The President's Climate Action Plan*, Washington, D.C. (June). Available at <https://www.whitehouse.gov/sites/default/files/image/president27sclimateactionplan.pdf>.

FEMA (Federal Emergency Management Agency), 2008, *IS-700.A—National Incident Management System (NIMS): An Introduction*. Available at <https://emilms.fema.gov/IS700aNEW/NIMS01summary.htm>.

Fugere, R., 2013, *PG&E Metcalf Incident and Substation Security*, CPUC Safety and Enforcement Division.

GAO (United States Government Accountability Office), 2014, *Climate Change – Energy Infrastructure Risks and Adaptation Efforts*, GAO-14-74, Report to Congressional Requesters. (January). Available at <http://www.gao.gov/assets/670/660558.pdf>.

IPCC (Intergovernmental Panel on Climate Change), 2012, *Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation*, Special Report of Working Groups I and II of the Intergovernmental Panel on Climate Change, edited by C.B. Field, V. Barros, T.F. Stocker, D. Qin, D.J. Dokken, K.L. Ebi, M.D. Mastrandrea, K.J. Mach, G.K. Plattner, S.K. Allen, M. Tignor, and P.M. Midgley, Cambridge, UK: Cambridge University Press. Available at <http://ipcc-wg2.gov/SREX/>.

ISO (International Standards Organization), 2012, *ISO 22301: Societal Security—Business Continuity Management Systems—Requirements* (May). Available at https://www.pea.co.th/BCM/DocLib/ISO_22301_2012.pdf.

Jones, E., 2013, *Enhancing Energy Resiliency to Natural Disasters: Key Findings from Recent Natural Disasters*, Pacific Northwest National Laboratory, for Department of Homeland Security Science & Technology Directorate (September). Available at http://export.gov/build/groups/public/@eg_main/@reee/documents/webcontent/eg_main_065305.pdf.

Kazamaa, M., and T. Noda, 2012, “Damage Statistics (Summary of the 2011 off the Pacific Coast of Tohoku Earthquake Damage),” *Soils and Foundations* 52(5):780–792.

Keogh, M., and C. Cody, 2013, *Resilience in Regulated Utilities*, NARUC Grants and Research, with support from DOE (November).

Lansing Board of Water and Light, 2014, Report on the Lansing Board of Water and Light's Response to the December 2013 Ice Storm, Community Review Team (May 5).

Lenfest, R., 2016, *A Remedy for False Security*. Available at <http://www.leedspathwest.com/a-remedy-for-false-security>.

Meade, 2015, Personal Communication.

Meade, 2016, Website, Chicago, IL. Available at <http://www.meade100.com/index.html>.

Michigan Public Service Commission (MPSC), 2014, *Staff Report December 2013 Ice Storm*, Electric Operations Section, Operations and Wholesale Markets Division (March 10).

Moeller, P., 2013, "Challenges of an Aging American Workforce," *U.S. News Money* (June 19). Available at <http://money.usnews.com/money/blogs/the-best-life/2013/06/19/challenges-of-an-aging-american-workforce>.

NARUC (National Association of Regulatory Utility Commissioners), 2016, *About NARUC*, Website. Available at <https://www.naruc.org/about-naruc/about-naruc/>.

NASA (National Aeronautics and Space Administration), 2009, "The Day the Sun Brought Darkness" (March 13). Available at http://www.nasa.gov/topics/earth/features/sun_darkness.html.

NASEO (National Association of State Energy Officials), 2016a, *About NASEO*, Website. Available at <https://www.naseo.org/about-naseo>.

NASEO, 2016b, *NASEO Committees*, Website. Available at <https://www.naseo.org/committees>.

National Infrastructure Protection Plan (NIPP) Energy Sector-Specific Plan, 2015. Available at <https://www.dhs.gov/publication/nipp-ssp-energy-2015>.

NERC (North American Electric Reliability Corporation), 2013, *GridEx*, Website. Available at <http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx>.

NERC, 2014, *Polar Vortex Review* (September). Available at http://www.nerc.com/pa/rrm/January%202014%20Polar%20Vortex%20Review/Polar_Vortex_Review_29_Sept_2014_Final.pdf.

NERC, 2015a, *Reliability and Accountability*, Website. Available at <http://www.nerc.com/Pages/default.aspx>.

NERC, 2015b, *State of Reliability Report 2015* (May). Available at <http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2015%20State%20of%20Reliability.pdf>.

NOAA (National Oceanic and Atmospheric Administration), 2013, *Service Assessment: The Historic Derecho of June 29, 2012*, National Weather Service, U.S. Department of Commerce (January). Available at <http://www.nws.noaa.gov/os/assessments/pdfs/derecho12.pdf>.

Oregon Seismic Safety Policy Advisory Commission, 2013, *The Oregon Resilience Plan: Reducing Risk and Improving Recovery for the Next Cascadia Earthquake and Tsunami*, Report to the 77th Legislative Assembly (February).

Parfomak, P.W., 2014, *Physical Security of the U.S. Power Grid: High Voltage Transformer Substations*, Congressional Research Service Report. Available at <https://www.fas.org/sgp/crs/homesecc/R43604.pdf>.

Pillon, J., 2015, Personal Communication.

PSE&G (Public Service Electric and Gas Company) Long Island, 2016a, Personal Communication.

PSE&G Long Island, 2016b, *Public Service Electric and Gas Company*, Website. Available at <https://www.pseg.com/family/pseandg/>.

PSE&G Long Island, 2016c, *About Us*, Website. Available at <https://www.PSEGLiny.com/page.cfm/AboutUs>.

PSE&G Long Island, 2016d, *PSE&G Long Island Further Strengthens Electric Grid: Resiliency Projects Protect the System from Extreme Weather*, Website. Available at <https://www.psegliny.com/page.cfm/AboutUs/PressReleases/2015/031415-FEMA>.

PwC (PricewaterhouseCoopers), 2013, *Power and Utilities Changing Workforce—Keeping the Lights on* (December). Available at <https://www.pwc.com/us/en/power-and-utilities/publications/assets/pwc-power-utilities-changing-workforce.pdf>.

Risky Business Project, 2014, *The Economic Risks of Climate Change in the United States: A Climate Risk Assessment for the United States* (June).

Sathayea, J.A., L.L. Dalea, P.H. Larsena, G.A. Fittsa, K. Koyc, S.M. Lewisd, and A.F.P. de Lucenae, 2013, *Estimating impacts of warming temperatures on California's electricity system*, *Global Environmental Change* 23(2): 499–511.

SHRM (Society for Human Resource Management), 2015, *The Aging Workforce—Basic and Applied Skills*, Society for Human Resource Management, Washington, D.C. Available at <http://www.shrm.org/research/surveyfindings/articles/pages/shrm-older-workers-basic-and-applied-skills.aspx>.

Smith, R., 2014, "Assault on California Power Station Raises Alarm on Potential for Terrorism: April Sniper Attack Knocked Out Substation, Raises Concern for Country's Power Grid," *The Wall Street Journal* (February 5).

Society for Human Resource Management, 2014, *SHRM and SHRM Foundation Launch Aging Workforce Project*, Press Release. Available at <https://www.shrm.org/about/pressroom/pressreleases/pages/agingworkforceprojectlaunch.aspx>.

U.S. Global Change Research Program, 2014, *Climate Change Impacts in the United States*, U.S. National Climate Assessment. Available at <http://nca2014.globalchange.gov/>.

Wang, Y., S.F. Bartlett, and S.B. Miles, 2012, *Earthquake Risk Study for Oregon's Critical Energy Infrastructure Hub*, prepared for Oregon Department of Energy and Oregon Public Utility Commission (August).

Wire, The, 2016, "Ice Has Weighty Effect on Power Lines." Available at <http://oppdthewire.com/effects-of-ice-on-power-lines/>.

This page intentionally left blank

Appendix A – Additional Information on Data Sources

A.1 Electric Utilities and Utility Contractors

A.1.1 Central Hudson Gas & Electric Corporation

Central Hudson Gas & Electric Corporation (Central Hudson) is a regulated transmission and distribution utility with approximately 300,000 electric customers and 79,000 natural gas customers. Central Hudson's territory is mix of small urban, suburban, and rural areas in the Hudson River Valley. The company's natural gas system consists of 165 miles of transmission pipelines and 1,229 miles of distribution pipelines. Its electric distribution system consists of 7,200 pole-miles of overhead lines and 1,500 trench-miles of underground lines, and the transmission system consists of 629 pole-miles of line.¹⁹¹ Central Hudson is currently working on improving transmission infrastructure and addressing known system congestion in the statewide electric grid to provide added economic, environmental, and reliability benefits to Central Hudson customers and all New Yorkers. This approach will also lead to lower-cost energy and renewable power upstate, particularly wind power, to flow more readily throughout New York.¹⁹²

A.1.2 Public Service Electric and Gas Company Long Island

Public Service Electric and Gas Company (PSE&G) is one of the nation's largest combined electric and gas companies, with approximately 1.8 million gas customers and 2.2 million electric customers. The service territory is 2,600 square miles, covering more than 300 urban, suburban, and rural communities across New Jersey.¹⁹³ PSE&G Long Island, a subsidiary of PSE&G, is a publicly traded energy company with \$11 billion in annual revenues that operates the Long Island Power Authority's transmission and distribution system under a 12-year contract.¹⁹⁴ PSE&G Long Island is in the process of implementing several improvement projects as part of a \$729 million federally funded, 3-year reliability and resiliency project to strengthen the electric grid across Long Island and in the Rockaways, and to improve its ability to withstand extreme weather events. Specific projects include plans to upgrade or replace more than 1,000 miles of mainline circuit facilities, elevate and protect flood-prone substations, and install innovative automation that isolates faults, all of which will allow PSE&G Long Island to limit the number of customers impacted by an outage and significantly speed up restoration if power is lost.¹⁹⁵

¹⁹¹ Central Hudson Gas & Electric Corporation, 2016b, *About Us: Our Mission Statement*, Website.

¹⁹² Central Hudson Gas & Electric Corporation, 2016c, *Projects*, Website.

¹⁹³ PSE&G Long Island, 2016b, *Public Service Electric and Gas Company*.

¹⁹⁴ PSE&G Long Island, 2016c, *About Us*, Website.

¹⁹⁵ PSE&G Long Island, 2016d. PSE&G Long Island, 2016d. PSE&G Long Island, 2016d, *PSE&G Long Island Further Strengthens Electric Grid: Resiliency Projects Protect the System from Extreme Weather*, Website.

A.1.3 Con Edison of New York

Con Edison of New York (Con Ed) is one of the nation's largest investor-owned energy companies, with approximately \$12 billion in annual revenues and \$40 billion in assets.¹⁹⁶ The company provides electricity, gas, and steam to more than 3 million customers in New York City and Westchester County, New York. The electrical system, said to be the world's most complex and most reliable electric power system, consists of almost 95,000 miles of underground cable, nearly 34,000 miles of overhead cable, and more than 90,000 transformers.¹⁹⁷ Con Edison is currently in the first year of a 4-year, \$1 billion storm-hardening program in the wake of 2012's Superstorm Sandy. More than 65,000 outages have been avoided as a result of investments made since the program began.¹⁹⁸

A.1.4 Meade Electric Co.

Meade Electric Co. (Meade) is a large utility contractor located in Chicago, Illinois. It specializes in the design, construction, and maintenance of electric power and natural gas distribution systems and telecommunications technologies.¹⁹⁹ For more than 100 years, Meade has worked with several electric utility companies, including Commonwealth Edison and Indianapolis Power & Light Company. With around 60 crews and in-house mechanics capabilities, Meade has extensive expertise in the restoration of storm-damaged systems. The company also has specific storm partnerships for coordinating additional restoration crews, who have supported utilities after hurricanes (e.g., Katrina and Ike) and during extreme winds and ice events in the Midwest.²⁰⁰

A.2 Publicly Available Sources

A.2.1 North American Electric Reliability Corporation and Federal Energy Regulatory Commission

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the reliability of the bulk power system in North America. NERC develops and enforces reliability standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organization for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes

¹⁹⁶ Con Edison, 2016b, *About Us*, Website.

¹⁹⁷ Con Edison, 2016c, *Facts and Background*, Website.

¹⁹⁸ Con Edison, 2016d, *Con Edison Wins 2015 ReliabilityOne™ Award for Outstanding System-Wide Reliability*.

¹⁹⁹ Meade, 2016, Website, Chicago, IL.

²⁰⁰ Ibid.

users, owners, and operators of the bulk power system, which serves more than 334 million people.²⁰¹

A.2.2 U.S. Department of Energy Office of Electricity Delivery and Energy Reliability

The U.S. Department of Energy Office of Electricity Delivery and Energy Reliability (DOE OE) provides national leadership to ensure that the nation's energy delivery system is secure, resilient, and reliable. Its work involves developing the federal and state electricity policies and programs that shape electricity system planning and market operations; developing new technologies to improve infrastructure; bolstering the resilience of the electric grid; and assisting with restoration when major energy supply interruptions occur.²⁰² The DOE OE, in collaboration with the National Association of State Energy Officials (NASEO), the National Association of Regulatory Utility Commissioners (NARUC), the National Conference of State Legislatures (NCSL), and the National Governors Association, also works closely with state and local governments on energy risk and assurance issues.²⁰³

Through the American Recovery and Reinvestment Act of 2009, the DOE OE was able to provide grants to state and local governments for energy assurance planning. Under this program, DOE OE awarded grants to states and local governments to enable those governments to develop or refine their energy assurance plans (EAPs), develop in-house expertise on infrastructure interdependencies and related vulnerabilities, and integrate renewable energy portfolios and new applications, such as cybersecurity and smart-grid technology, into their energy assurance planning.^{204,205} Funds were provided to 47 states, the District of Columbia, 2 territories, and 43 cities to develop new or refine existing EAPs, which contribute to the resilience of the Energy Sector by focusing on the entire energy supply system.²⁰⁶ These plans were largely completed between 2013 and 2014. Since that time, there has not been any additional federal funding to update these plans despite requests included in the president's budget proposals in fiscal years 2016 and 2017.

A.2.3 Quadrennial Energy Review

Informed by the June 2013 President's *Climate Action Plan* and in response to a 2011 recommendation by the President's Council of Advisors on Science and Technology, the Administration-wide Quadrennial Energy Review (QER) enables the federal government to translate policy goals into a set of analytically based, integrated actions (e.g., executive actions, legislative proposals, and budget and resource requirements for proposed investments) over a

²⁰¹ NERC, 2015a, *Reliability and Accountability*, Website.

²⁰² DOE OE, 2015b, *About Us*, Website.

²⁰³ DOE OE, 2015c, *State and Regional Energy Risk Assessment Initiative—State Energy Risk Profiles*, Website.

²⁰⁴ DOE OE, 2015d, *State and Local Energy Assurance Planning*, Website.

²⁰⁵ DOE EPSA, 2015.

²⁰⁶ DOE OE, 2012, *American Recovery and Reinvestment Act Energy Assurance Planning Bulletin*, Vol. 4, No. 4.

4-year planning horizon. In April 2015, the QER task force provided the first QER report: *Energy Transmission, Storage, and Distribution Infrastructure*, which examined the nation's infrastructure for transmission, storage, and distribution, including liquid and natural gas pipelines, the grid, and shared transport, such as rail, waterways, and ports. The QER report also recommended support for the updating and expansion of the state EAPs. On the basis of the findings in the first installment of the QER, the administration directed the second installment of the QER to include a set of findings and policy recommendations to help guide the modernization of the nation's electric grid and ensure its continued reliability, safety, security, affordability, and environmental performance through 2040.²⁰⁷

A.2.4 National Association of State Energy Officials

The NASEO is the only national nonprofit association for the governor-designated energy officials from each of the 56 states and territories. Formed by the states in 1986, NASEO facilitates peer learning among state energy officials, serves as a resource for and about state energy offices, and advocates the interests of the state energy offices to Congress and federal agencies.²⁰⁸ NASEO committees are the formal mechanism for members to work on key priorities and ongoing issues. The primary role of the committees is to identify emerging issues relevant to the state and territory energy offices and to collect, analyze, and disseminate this information to educate members and others. The committees' work helps to guide the association's strategic direction and, where appropriate, build consensus on pertinent issues.²⁰⁹ NASEO's Energy Security Committee is responsible for energy assurance planning and preparedness and serves as a focal point for providing technical support to states.

A.2.5 National Association of Regulatory Utility Commissioners

NARUC is a nonprofit organization that represents the state public service commissions that regulate energy, telecommunications, water, and transportation utilities. NARUC currently has 69 state and federal regulatory agencies, 258 commissioners, and 8 vacancies, representing all 50 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. NARUC's mission is to serve in the public interest by improving the quality and effectiveness of public utility regulation. Its members, under state law, have an obligation to ensure the establishment and maintenance of utility services and that such services are provided at fair, reasonable, and non-discriminatory rates.²¹⁰

²⁰⁷ DOE EPISA, 2016, *About the Quadrennial Energy Review*, Website.

²⁰⁸ NASEO, 2016a, *About NASEO*, Website.

²⁰⁹ NASEO, 2016b, *NASEO Committees*, Website.

²¹⁰ NARUC, 2016, *About NARUC*, Website.

A.2.6 Electric Power Research Institute

The Electric Power Research Institute (EPRI) is a nonprofit organization that conducts research and development relating to the generation, delivery, and use of electricity. Its members consist of more than 1,000 organizations, including electric utilities, firms, government agencies, corporations, and public or private entities. EPRI's research primarily focuses on developing ways to enable power systems to be more flexible, resilient, and connected.²¹¹

A.2.7 Edison Electric Institute

The Edison Electric Institute (EEI) is the association that represents all U.S. investor-owned electric companies. Its members provide electricity for 220 million Americans, operate in all 50 states and the District of Columbia, and directly employ more than 500,000 workers. EEI's mission is to ensure its members' success by advocating public policy, expanding market opportunities, and providing strategic business information.²¹²

²¹¹ EPRI, 2016, *Our Members*, Website.

²¹² Edison Electric Institute, 2016, Website.

This page intentionally left blank

Appendix B – Detailed Information on Electric Grid Threats and Vulnerabilities

B.1 Natural Hazards and Climate Change

Currently, extreme weather events are the largest source of damage to grid infrastructure and disturbances to electric power service.²¹³ An increase in the frequency and magnitude of disruptive extreme weather events is the primary way in which climate change is expected to further impact energy infrastructure. Although climate change impacts are projected to vary regionally, emerging and continuing trends that have been observed and attributed to climate change include more frequent and more intense storm events, heat waves, droughts, wildfires, changing precipitation patterns, and coastal flooding. In addition, sea-level rise will exacerbate the potential for climate change to bring more frequent and stronger hurricanes and higher storm surges.^{214,215} Further, regional variation in climate change impacts does not imply regional isolation. As systems have become increasingly interconnected, impacts that occur on a local or regional level often have broader implications. For example, climate impacts felt in one region may put pressure on the electric power grid elsewhere to compensate for those changes.²¹⁶

The part of the electricity infrastructure that is the most vulnerable to natural hazard and climate change effects is the transmission and distribution grid, although about 90 percent of disruptions typically occur along the more localized distribution systems²¹⁷ because transmission towers tend to be more structurally sturdy. Multiple utilities specifically identified trees and limbs falling on utility infrastructure as a critical threat to the overhead electric distribution system.^{218,219,220} This is also in part because the United States possesses considerable excess power generation capacity (i.e., 10 percent–15 percent reserve required by federal regulations), which is generally sufficient to avoid disruption within generation.^{221,222}

²¹³ DOE EPSA, 2015.

²¹⁴ Ibid.

²¹⁵ GAO, 2014.

²¹⁶ DOE, 2013, *U.S. Energy Sector Vulnerabilities to Climate Change and Extreme Weather*, DOE/PI-0013 (July).

²¹⁷ DOE OE, 2010.

²¹⁸ Con Edison, 2016a.

²¹⁹ Central Hudson Gas & Electric Corporation, 2016a.

²²⁰ PSE&G Long Island, 2016a.

²²¹ DOE OE, 2010.

²²² Barrett et al., 2013.

B.1.1 Ice, Snow, and Extreme Cold Weather

In winter, dense snow and ice accumulation are key threats to electricity transmission and distribution,²²³ primarily because of the added weight to the towers, poles, and lines, as well as an increased risk from trees and storm-related wind. It is reported that one-quarter inch of ice can increase the weight of a tree branch to 30 times its normal weight, causing it to break; one-half inch of ice is the equivalent of 500 pounds of weight on a single power line span.²²⁴ This added weight can cause distribution towers to collapse, distribution poles to crack, and lines to sag and break.^{225,226} In addition, ice stays on the electrical lines and trees until the sun melts it or the temperature rises above 32°F, which results in additional outages and hindrance of restoration efforts after a storm has passed. Only after the ice melts, and the additional load is removed, is the risk of further damage to the system and further outages reduced. To illustrate the extent of potential damage, a major ice storm (the third largest on record) hit the mid-section of lower Michigan in December 2013. The storm resulted in an estimated 630,000 customers without power to their homes and/or businesses for as long as 8 to 11 days.^{227,228,229} Figure B.1 shows some of the consequences from the December 2013 ice storm.²³⁰ During the previous winter, in February 2013, more than 660,000 customers lost power across eight states when the Northeast was affected by a winter storm that brought snow, heavy winds, and coastal flooding to the region.²³¹ Crippled transportation networks can further hinder repair and restoration efforts.



Figure B.1 December 2013 Ice Storm in Lower Michigan

Cold temperatures also can be dangerous for utility personnel and can stress equipment that is not designed to withstand such extremes. In January 2014, the Midwest, South Central, and East Coast regions of North America experienced a polar vortex, where extreme cold weather conditions occurred in lower latitudes than normal, resulting in temperatures 20°F to 30°F below

²²³ Central Hudson Gas & Electric Corporation, 2016a.

²²⁴ DTE Electric Company, 2014.

²²⁵ Lenfest, R., 2016, *A Remedy for False Security*.

²²⁶ The Wire, 2016, *Ice has weighty effect on power lines*.

²²⁷ DTE Electric Company, 2014.

²²⁸ Consumers Energy, 2014, *Consumers Energy Company's Report in Response to MPSC Order in Case No. U-17542* (February 7).

²²⁹ Lansing Board of Water and Light, 2014, *Report on the Lansing Board of Water and Light's Response to the December 2013 Ice Storm*, Community Review Team (May 5).

²³⁰ Michigan Public Service Commission (MPSC), 2014, *Staff Report December 2013 Ice Storm*, Electric Operations Section, Operations and Wholesale Markets Division (March 10).

²³¹ DOE, 2013.

average. Some areas faced multiple days that were 35°F or more below their average temperatures.²³² The frigid cold temperatures associated with the polar vortex resulted in record-high winter peak electrical demands, with some areas registering at almost 18 percent greater than the previous all-time winter peak.²³³ Frozen equipment was identified as the leading cause of power outages, as temperatures fell well below the design bases. On the generation side of the grid, an extra demand for heating gas or oil during cold periods, combined with potentially crippled transportation networks, can put a fossil fuel power plant's fuel source delivery at risk. In addition, certain fuel sources (e.g., coal) can freeze during transport or while in the storage yard, rendering them temporarily unusable; natural gas wells also have the potential to freeze and disrupt supply.

B.1.2 Thunderstorms, Tornadoes, and Hurricane-Force Winds

In spring and summer, thunderstorms, tornadoes, and hurricanes directly (e.g., high winds or lightning) and indirectly (e.g., trees or flying debris) cause damage to buildings and exposed infrastructure elements (e.g., towers, poles, transformers, and power lines) throughout the grid. Most vulnerable are the transmission and distribution systems, because towers, poles, and power lines commonly fall, break, touch, or short out. Uprooted trees can even take out underground utility lines. Hurricane-force winds are explicitly credited as another primary cause of damage to the electric grid, particularly the transmission and distribution infrastructure. Resulting power disruptions can often be long term if the ensuing damage takes on a domino effect, knocking out trees, transmission towers, transformers, and distribution poles together.²³⁴ For example, in June 2012, an estimated 4 million people and businesses lost power for up to 1 week when a complex of thunderstorms, coupled with widespread strong winds (i.e., a derecho), swept across the Midwest to the Mid-Atlantic coast, affecting 10 states and Washington, D.C.^{235,236}

Storm-related outages, which individually can last from minutes to weeks, have been estimated to cost the U.S. economy an inflation-adjusted average of \$18 billion to \$33 billion per year between 2003 and 2012; some estimates are even greater.²³⁷ Available damage and outage figures for specific coastal storms include Superstorm Sandy (2012) at \$8 billion and 14 days; Hurricane Isabel (2003) at \$6.5 billion and 14 days; and Hurricane Irene (2011) at \$6 billion and 5 days.²³⁸

²³² NERC, 2015b, *State of Reliability Report 2015* (May).

²³³ NERC, 2014, *Polar Vortex Review* (September).

²³⁴ DOE OE, 2010.

²³⁵ DOE, 2013.

²³⁶ NOAA (National Oceanic and Atmospheric Administration), 2013, *Service Assessment: The Historic Derecho of June 29, 2012*, National Weather Service, U.S. Department of Commerce (January).

²³⁷ DOE EPSA, 2015.

²³⁸ Jones, E., 2013, *Enhancing Energy Resiliency to Natural Disasters: Key Findings from Recent Natural Disasters*, Pacific Northwest National Laboratory, for DHS Science and Technology Directorate (September).

B.1.3 Increasing Temperature and Extreme Hot Weather

The manifestation of extreme hot weather can push infrastructure beyond its design limitations. Consequently, increased summer air temperatures and number of extreme heat days are commonly identified as significant threats to the transmission and distribution system.^{239,240,241} During extreme heat conditions, electricity lines experience reduced current-carrying capacity, increased stress, and thermal expansion, which can cause lines to sag and come into contact with trees. Systems and equipment also operate less efficiently and have great potential to malfunction, leading to power interruptions and outages.^{242,243,244} For example, during a July 2006 heat wave, more than 2,000 distribution line transformers in California failed, causing loss of power to approximately 1.3 million customers.²⁴⁵ Taking into account future climate change impacts on temperature, a study of the California power grid projected that during the hot periods of August 2100 (under a higher emissions scenario) a 9°F (5°C) increase in air temperature could decrease transmission line capacity by 7 percent to 8 percent and cause substation capacity to fall by 2 percent to 4 percent, although these capacity losses could be reduced by modifying future operating practices and system designs.²⁴⁶ The effects of hot weather may be further intensified by low wind speeds and elevated nighttime temperatures, which would prevent transmission lines from cooling.²⁴⁷



Figure B.2 Wildfire Damage to Electric Distribution System Wood Poles

Extreme hot weather can further lead to severe and prolonged drought conditions and an increased risk of wildfires. The heat, smoke, and particulate matter can also impact the capacity of transmission lines and devastate distribution systems, burning down poles and leaving cables lying on the ground,²⁴⁸ as illustrated in Figure B.2.²⁴⁹ In the summer of 2011, severe drought and record wildfires in Arizona and New Mexico burned more than 1 million acres and threatened the DOE's Los Alamos National Laboratory, as well

²³⁹ Con Edison, 2016a.

²⁴⁰ PSE&G Long Island, 2016a.

²⁴¹ DOE EPSA, 2015.

²⁴² DOE EPSA, 2015.

²⁴³ DOE, 2013.

²⁴⁴ Barrett et al., 2013.

²⁴⁵ DOE, 2013.

²⁴⁶ Sathayea, J.A., L.L. Dalea, P.H. Larsena, G.A. Fittsa, K. Koyc, S.M. Lewis, and A.F.P. de Lucenae, 2013, "Estimating Impacts of Warming Temperatures on California's Electricity System," *Global Environmental Change* 23(2): 499–511.

²⁴⁷ DOE, 2013.

²⁴⁸ Ibid.

²⁴⁹ *T&D World Magazine*, 2014, "Crews Repair Transmission Lines after Washington Wildfire" (June 26).

as two high-voltage lines transmitting electricity from Arizona to approximately 400,000 customers in New Mexico and Texas.²⁵⁰

Higher temperatures also commonly manifest themselves as a greater peak electric demand for cooling, which increases stress on the already burdened system. Increasing air and water temperatures can also put electric power plants at risk by reducing cooling efficiency, increasing the likelihood of exceeding thermal effluent limits that protect local ecology, and increasing the potential risk of partial or full shutdowns of generation facilities.²⁵¹ Furthermore, depending on their source of cooling water, electric power plants are also potentially vulnerable to decreasing water availability. For example, in 2014, during the decade-long extreme drought in Texas, a gas turbine electric facility had to be taken offline because the water levels in its lake, which served as its sole source of cooling water, fell below the plant's intake structures.²⁵² During the summer of 2010, water levels in Nevada's Lake Mead dropped to elevations not seen since 1956, prompting the Bureau of Reclamation to reduce Hoover Dam's thermoelectric power generating capacity by 23 percent, which created concerns around destabilization of the Southwest energy markets.²⁵³

B.1.4 Storm Surges, Flooding, and Increased Precipitation

The complexities associated with shifting atmospheric conditions, in the face of increasing temperatures from climate change, will likely lead to a rise in sea levels, an increase in tropical storm and hurricane activity (i.e., intensity, frequency, or duration), and a shift in extratropical storm tracks.²⁵⁴ In coastal areas, more intense storm events, combined with sea-level rise and sometimes coupled with coastal subsidence, will together contribute to greater storm surge and wave action impacts that can infiltrate, damage, and flood out distribution networks and substations, transmission structures, and power plants.^{255,256,257} In addition, salt water can be very corrosive to metal and increase the level of damage to switching and other equipment. The resulting effects of a Superstorm Sandy in 2012 led to more than 8 million customers without power and total loss estimates²⁵⁸ on the order of \$65 million, reflecting direct effects of

²⁵⁰ DOE, 2013.

²⁵¹ Ibid.

²⁵² Barringer, F., 2015, "Troubling Interdependency of Water and Power," *The New York Times*, Energy & Environment (April 22).

²⁵³ DOE, 2013.

²⁵⁴ IPCC, 2012.

²⁵⁵ DOE EPSA, 2015.

²⁵⁶ DOE OE, 2010.

²⁵⁷ GAO, 2014.

²⁵⁸ Since 1980, National Oceanic and Atmospheric Administration's National Climatic Data Center has provided aggregated loss estimates for major weather and climate events, including tropical cyclones, floods, droughts, heat waves, severe local storms (e.g., tornado, hail, wind damage), wildfires, crop freeze events, and winter storms. Estimates include physical damage to buildings; material assets; time element losses, such as hotel costs for loss of living quarters; vehicles; public and private infrastructure; and agricultural assets (e.g., buildings, machinery, livestock). Estimates do not include losses to natural capital/assets, health-care-related losses, or values associated with loss of life.

weather/climate events and representing both insured and uninsured losses.²⁵⁹ Overall, storm surge and associated flooding generally cause more devastation than hurricane-force winds, both in terms of infrastructure and human life.²⁶⁰ Looking to the future, economic research has predicted that within the next 15 years, sea-level rise, combined with increased storm surge, will likely increase the average cost of coastal storms along the Eastern Seaboard and Gulf of Mexico by \$2 billion to \$3.5 billion per year. Coupled with potential changes in hurricane activity, the likely rise in average losses could increase to an estimated \$7.3 billion per year.²⁶¹

As air temperatures increase, the water-holding capacity of the also air increases, which causes a change in the timing and amount of precipitation. Overall, average U.S. precipitation has increased since 1900, although some areas have had increases greater than the national average, and some areas have had decreases. In this century, climate models generally predict more winter and spring precipitation for the northern United States, and less for the Southwest.²⁶²

The resulting precipitation is manifesting as more frequent and intense downpours, with a greater proportion of total rainfall coming from heavy precipitation, which consequently increases the frequency, intensity, and duration of flooding.²⁶³ Increased precipitation also creates a soil structure that is more commonly saturated,^{264,265} which can weaken foundations of infrastructure elements and further increase their risk of damage from extreme weather events. Flash flooding can also wipe out infrastructure elements, as well as create the potential for dam overflow, bypass, or failure.

It is important to add that, although flooding most commonly results from extreme weather events, it also occurs for other reasons (e.g., dam/levy failure). Regardless of the cause, flooding is one of the few natural-based phenomena that can directly affect generation facilities.^{266,267}

B.1.5 Earthquakes

Any earthquake event has the potential to cause physical damage to buildings and lifeline infrastructure, but the larger the earthquake, the greater the resulting impacts. In addition to earthquake size, impact will depend on region and how seismic considerations are to be addressed in facility, building, and infrastructure (e.g., tower) design. For example, the 9.0-magnitude subduction zone earthquake, which occurred in Japan in March 2011, resulted in nearly 22,000 missing or dead people, approximately 4.4 million homes experiencing power

²⁵⁹ GAO, 2014.

²⁶⁰ DOE OE, 2010.

²⁶¹ Risky Business Project, 2014, *The Economic Risks of Climate Change in the United States: A Climate Risk Assessment for the United States* (June).

²⁶² U.S. Global Change Research Program, 2014, *Climate Change Impacts in the United States*, U.S. National Climate Assessment.

²⁶³ DOE, 2013.

²⁶⁴ Con Edison, 2016a.

²⁶⁵ PSE&G Long Island, 2016a.

²⁶⁶ Con Edison, 2016a.

²⁶⁷ PSE&G Long Island, 2016a.

outages, and extensive physical damage to the electric infrastructure that took months (or longer) to recover.²⁶⁸ The damage the earthquake caused to power plants and substations, combined with the associated tsunami, aftershocks, and ground failure (e.g., liquefaction and lateral spreading), included collapsed or tilting structures; flooding; liquefaction; exposure of foundation piles; and damage to transformers, breakers, isolators, and fuel unloaders. Impacts on electric transmission and distribution systems included damage to connections in buried structures; loss, damage, collapse, or tilting of electric power towers and poles; and loss, breakage, or downing of cables and power lines.²⁶⁹ If a similar large-magnitude earthquake and tsunami occurred in Oregon, which has critical energy infrastructure located in an area of significant seismic hazard, research shows that consequences would likely include thousands of deaths, damage across critical infrastructure sectors (e.g., transportation, energy, telecommunications, and water/wastewater systems), and economic losses exceeding \$30 billion.^{270,271}

B.2 Direct Intentional Attacks

B.2.1 Physical Attacks

Electric transmission and distribution systems are traditionally open and cover long distances, making them extremely vulnerable to an ever-expanding range of direct physical attacks, from acts of vandalism or minor theft to deliberate and coordinated destruction of equipment and facilities.^{272,273} However, power plant facilities and associated infrastructure are also potentially vulnerable. Malicious actors carrying out these attacks encompass a wide range of potential offenders, including terrorist organizations, international enemy states, economically or otherwise competing nations, lone-wolf anarchists, disgruntled employees, and/or mischievous individuals.²⁷⁴

The potential loss of system functionality caused by physical attacks can result in instability, uncontrolled separation, and cascading failures.²⁷⁵ Thus, while attacks like these may seem unlikely, and the majority do not result in widespread blackouts, their intent and potential severe consequences highlight them as a key threat. For example, a targeted attack against one or a few key nodes could have a significant disproportionate impact throughout the system, as was

²⁶⁸ Kazamaa, M., and T. Noda, 2012, “Damage Statistics (Summary of the 2011 off the Pacific Coast of Tohoku Earthquake Damage),” *Soils and Foundations* 52(5):780–792.

²⁶⁹ Kazamaa and Noda, 2012.

²⁷⁰ Wang, Y., S.F. Bartlett, and S.B. Miles, 2012, *Earthquake Risk Study for Oregon’s Critical Energy Infrastructure Hub*, prepared for Oregon Department of Energy and Oregon Public Utility Commission (August).

²⁷¹ Oregon Seismic Safety Policy Advisory Commission, 2013, *The Oregon Resilience Plan: Reducing Risk and Improving Recovery for the Next Cascadia Earthquake and Tsunami*, Report to the 77th Legislative Assembly (February).

²⁷² DOE EPSA, 2015.

²⁷³ Meade, 2015.

²⁷⁴ Barrett et al., 2013.

²⁷⁵ DOE EPSA, 2015.

potentially the case in San Jose, California, in April 2013 when PG&E Company's Metcalf Transmission Substation was attacked by gunfire. The targeted substation is a critical node in supplying electric power to the Silicon Valley, headquarters to some of the largest technological corporations in the world (e.g., Intel, Google, Facebook, and SanDisc, to name a few). The gunshots resulted in the release of approximately 52,000 gallons of oil, which caused 17 transformers to overheat and shut down.²⁷⁶ Although power was successfully rerouted around the substation and customers did not lose power in the adjacent Silicon Valley area, an extended power outage to this area could have led to wide-ranging economic consequences. Nonetheless, an estimated \$15.4 million and 27 days were spent on restoration efforts to repair the damage and bring the substation back into operation.²⁷⁷

B.2.2 Cyber Attacks

From 2011 through 2014, there were few reported cyber incidents on the electric grid and none reported that resulted in system outages.²⁷⁸ However, the U.S. Department of Homeland Security (DHS) reports that cyber attacks on the electric grid system are increasing in both frequency and sophistication.²⁷⁹ As with direct physical attacks, cyber threats come from a variety of different sources, from individuals to organized criminal groups to nation states. The nature of cyber threats crosscuts everything. The most frequent type of intrusion is from adversaries who want to exploit or steal something of value (e.g., money or intellectual property), which can be sold without anyone knowing they were in the system. At the other extreme of the threat scale would be the risk of a terrorist or other enemy using cyber capabilities to attack, take over, and/or shut down electric power system controls, which could cause significant and far-reaching impacts across multiple critical infrastructure sectors.

In general, it is currently easier to "take down the grid" with a physical attack compared to a cyber attack. Over the past two decades, however, electricity system hardware and infrastructure technology (IT) infrastructure have become more interdependent, relying heavily on automation, sensor technology, centralized control of equipment, and high-speed communications to increase efficiency and improve awareness.²⁸⁰ This increased interdependence and system autonomy presents new vulnerabilities, which include exploitation of software vulnerabilities to penetrate utilities operating system security and targeted social engineering (e.g., phishing attacks). In general, the most critical systems at risk for cyber attacks are the supervisory control and data acquisition (SCADA) systems, which gather real-time measurements from substations and send out control signals to equipment, such as circuit breakers. If breached, hackers could manipulate SCADA systems and smart-grid technology to

²⁷⁶ Smith, R., 2014, "Assault on California Power Station Raises Alarm on Potential for Terrorism: April Sniper Attack Knocked Out Substation, Raises Concern for Country's Power Grid," *The Wall Street Journal* (February 5).

²⁷⁷ Fugere, R., 2013, *PG&E Metcalf Incident and Substation Security*, CPUC Safety and Enforcement Division.

²⁷⁸ DOE EPSA, 2015.

²⁷⁹ Bipartisan Policy Center, 2014, *Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat*, A Report from the Co-chairs of the Bipartisan Policy Center's Electric Grid Cybersecurity Initiative (February).

²⁸⁰ DOE EPSA, 2015.

disrupt the flow of electricity, transmit erroneous signals to operators, block the flow of vital information, cut off communications, disable protective systems, and even impart physical damage on facilities. As a result, there is growing concern over the “hack-ability” of U.S. electric power grid system and software, which has the potential to quickly disrupt the electrical supply system and cripple the U.S. economy.

It is important to add that the convergence and application of new technology also provide opportunities for new grid-associated value streams, enhanced system performance, and more options for consumer interaction with electricity systems (as described in Section 4).

B.3 Geomagnetic and Electromagnetic Pulses

Another threat to critical electric power infrastructure is a geomagnetic or electromagnetic pulse (GMP or EMP), which is a sudden burst of electromagnetic radiation resulting from a natural or man-made event. Natural GMP events are generated from geomagnetic storms, which arise from the interaction between the solar activity and the Earth’s magnetic field and can occur on a worldwide scale. Geomagnetic storms produce high currents in the magnetosphere, which induces high currents in power lines, blowing out electric transformers and power stations. This type of event is most likely to happen at high latitudes, where the induced currents are greatest, or in regions that have long power lines where the ground is poorly conducting. The space weather scientific community generally agrees that a severe solar storm—capable of generating a GMP that would impact most high-voltage transformers and damage other critical grid assets over large geographic areas—will happen with a 100 percent certainty.^{281,282} Experts further predict a 12 percent chance of this GMP occurrence in the next 10 years and a 50 percent chance in the next 50 years. Ordinary low-level solar storms, which cause harmonics on the power lines, are already leading to significant damage to customer equipment and generating billions of dollars in annual insurance claims in the United States.²⁸³

Man-made electromagnetic effects can be generated by a nuclear explosion 25 to 250 miles above the Earth’s surface—high enough that the blast would not damage buildings or spread a lethal radioactive cloud, but still capable of creating a pulse that would fan out hundreds of miles. Alternately, a smaller, localized EMP device could be built using readily available materials and equipment from local or online electronics retailers.

The immediate effect of a GMP or EMP would resemble a blackout. Unlike blackouts, which can be restored relatively quickly, however, electromagnetic effects could severely damage or permanently destroy power systems, leaving them inoperable for months or longer. Of specific concern is a severe geomagnetic storm that could have a large geographic footprint and last for many hours (or sometimes days), which would lead to considerable, wide-scale equipment damage and long-term outages to major portions of the electric grid. The economic and societal

²⁸¹ DOE EPSA, 2015.

²⁸² Emprimus, 2015, *Effects of GMD & EMP on the State of Maine Power Grid*, prepared in partnership with Central Maine Power, Emera, Maine.

²⁸³ Ibid.

costs attributable to the consequences of this type of event could be substantial. For example, a geomagnetic storm in March 1989 resulted in a 12-hour blackout of the entire Province of Quebec, which included Montreal. The Quebec Blackout affected millions of people and went far beyond its borders, in that some U.S. electrical utilities lost part of their service supply. The New England Power Pool lost 1,410 megawatts (MW) as soon as the Quebec power grid went down; New York Power lost 150 MW. Across the United States from coast to coast, more than 200 power grid problems erupted within minutes of the start of storm. Fortunately, the nation had just enough power to spare, and no additional blackouts resulted.²⁸⁴

B.4 Aging Infrastructure

The U.S. system of generation, transmission, and distribution facilities was built over the course of more than a century; thus, the ages, conditions, and capacities of infrastructure vary greatly across the grid. Centralized electric generating plants with local distribution networks were started in the 1880s, and the grid of interconnected transmission lines was initiated in the 1920s. Taken altogether, the grid represents a complex patchwork of regional and local power plants, lines, and transformers that have widely differing ages, conditions, and capacities. For example, about 51 percent of the nation's generating capacity is in plants that were at least 30 years old at the end of 2010. While most gas-fired capacity is less than 10 years old, 73 percent of all coal-fired capacity is 30 years old or older. Most major dams, reservoirs, and hydroelectric plants in the United States (typically federally owned and operated) are 60 or more years old. Maintaining key features and functions of these power plants requires ongoing monitoring, maintenance, modernization, and rehabilitation of these structures and their component systems. Furthermore, nationally 70 percent of the nation's transmission lines and power transformers are 25 years or older, and 60 percent of circuit breakers are more than 30 years old.^{285,286} In some parts of the country, electric infrastructure may be more than 100 years old.²⁸⁷

Many of the key elements that make up the U.S. electric grid have been repaired, strengthened, and reinforced over the years, but rarely redesigned or fully modernized. This practice leads to lost power quality, productivity, and availability resulting from failures and outages due to practical issues like system fatigue, equipment malfunction, capacity bottlenecks, and misalignment of the system with how power is consumed today.^{288,289} Aging infrastructure is also more susceptible than newer assets to failure as a result of extreme weather-related hazards.²⁹⁰ It has been estimated that some 20 percent of the sustained outages (i.e., defined as those lasting more than 1 minute) were caused by failing electrical equipment.²⁹¹

²⁸⁴ NASA (National Aeronautics and Space Administration), 2009, "The Day the Sun Brought Darkness" (March 13).

²⁸⁵ ASCE, 2013.

²⁸⁶ Barrett et al., 2013.

²⁸⁷ DOE OE, 2010.

²⁸⁸ Barrett et al., 2013.

²⁸⁹ ASCE, 2013.

²⁹⁰ DOE OE, 2010.

²⁹¹ Barrett et al., 2013.

B.5 Capacity Constraints

Today, the electric power industry faces an ever-increasing demand for power as a result of growth in both population and in per-person power consumption. In the near term, the supply appears to be close to adequate to meet demand, although the system frequently operates at or near absolute peak capacity.²⁹² However, nationwide estimates have placed projected electricity demand increases around 0.8 percent per year, totaling around 20 percent through 2040.²⁹³ This over-demand, coupled with the limited capacity of older equipment, creates congestion points throughout the grid that can lead to curtailments, rotating blackouts, and system failures and inherently raises the risk of more and larger cascading blackouts.^{294,295} In addition, heat can build up in transmission lines as the current increases and, if a line fails, the current must be redirected through other interconnected lines in the grid. This rerouting, which can often be a result of aging transmission infrastructure, can overload circuits, requiring load shedding or risking a cascading collapse, depending on local system architecture.²⁹⁶

A reliable electricity generation system must have more capacity resources than anticipated peak demand to account for unanticipated outages and higher-than-anticipated peak demand. Under governance regimes, each system is required to operate at an excess capacity of 10 percent to 15 percent greater than the anticipated peak demand. Because of increased demand, however, some areas already fail to meet those standards. Resolving the mismatch between peak demand and available capacity will require either additional power generation in terms of new or expanded power plants or better management of current usage levels by spreading out demand across nonpeak hours—a main driver behind the idea of the smart grid.²⁹⁷ The use of smart-grid technology communicates with commercial, industrial, and residential customers about peak demand times and gives them the option (or not) to reduce their electric power use during these periods (i.e., during hot summer months).

B.6 Workforce Turnover and Loss of Institutional Knowledge

A solid talent base of skilled linemen, engineers, and operators is critical for maintaining operability and promoting sustainable growth in the electric power industry. However, the current and rapidly evolving workforce within the industry is creating safety, capability, and continuity challenges for utilities. The key issues are related to increasing turnover rates and loss of institutional knowledge.^{298,299} In general, as the economy continues to strengthen, the available range of job options widens, and turnover rates inevitably rise. In addition, younger generation high performers have a greater propensity to change jobs, as opposed to traditional

²⁹² Ibid.

²⁹³ EIA (U.S. Energy Information Administration), 2015, *Annual Energy Outlook 2015: With Projections to 2040*, DOE/EIA-0383(2015), DOE Office of Integrated and International Energy Analysis (April).

²⁹⁴ ASCE, 2013.

²⁹⁵ Barrett et al., 2013.

²⁹⁶ Meade, 2015.

²⁹⁷ Barrett et al., 2013.

²⁹⁸ Meade, 2015.

²⁹⁹ PwC, 2013.

utility workers who worked their way up with a company and normally settled in for the long term. Thus, as the rapidly aging utility workforce begins to retire (often due to diminished incentives to stay), demand will outpace supply because fewer young qualified people are ready and able to replace experienced workers. Furthermore, the training and development of new skilled personnel requires a long lead time, as on-the-job experience is essential to the knowledge transfer process.^{300,301} Taken together, these issues translate into a widening talent gap and loss of overall institutional knowledge that is threatening the continuity and resilience of the electric utility industry and increasing the likelihood of human error.

Increased retirement and turnover rates also have negative economic impacts on utility companies. For example, pension packages typically offered by utilities can be extremely generous, offering as much as 80 percent of an employee's final salary (or the average of their last few years' salary) plus all, or nearly all, of their medical benefits.³⁰² So, in addition to continually paying out these sums, utilities must also pay benefits for the replacement employees coming in, specifically increasing costs of medical benefits. This dynamic is further exacerbated if the utility needs to make multiple attempts at replacing the same positions due to turnover. As a result, overall productivity is affected, and acquisition costs are repeated.³⁰³

B.7 Human Error

The complex systems built and operated by humans across the grid are vulnerable to impacts resulting from or attributed to human-related mistakes or issues. For example, the August 2003 Northeastern blackout, which affected an estimated 50 million people in the Midwest, Northeast, and Ontario for 4 to 7 days, was in part attributed to set of human-related issues and mistakes. In general, the human failures included not determining and understanding inadequacies with respect to voltage instability, not establishing and monitoring appropriate transmission constraints, not adequately managing tree growth along transmission rights of way, and not having the proper data and systems to detect and be aware of the situation as it unfolded.³⁰⁴ Additional factors that contributed to the 2003 blackout include inadequate interregional visibility over the power system, dysfunction of a control area's data system, and lack of adequate backup capability to that system.³⁰⁵

B.8 Dependencies and Supply Chain Interruptions

Another area for consideration is systemic dependencies and potential impacts from other critical infrastructure disruptions. For example, natural gas and coal are used as fuels for power

³⁰⁰ Meade, 2015.

³⁰¹ DOE, 2006.

³⁰² PwC, 2013.

³⁰³ Ibid.

³⁰⁴ DOE EPSA, 2015.

³⁰⁵ Apt, J., L.B. Lave, S. Talukdar, M.G. Morgan, and M. Ilic, 2004, "Electrical Blackouts: A Systemic Problem," *Issues in Science and Technology* 20(4): 55–61 (Summer).

generation and grid operations; petroleum is used if required to maintain service fleets. Transportation networks (e.g., roads, pipelines, rail, waterways) are important in transporting fuel and raw materials to power plants and mobilizing repair crews after an event. Water is critical to thermoelectric fossil fuel power plants and some renewable plants (e.g., concentrated solar and biomass) for operation and cooling activities. Telecommunication systems are essential for monitoring and managing the electric grid via substations and control centers; they are also essential to the proper function of smart-grid technologies. Thus, the systems that supply and move resources to and from electric power plants are particularly critical, especially during an emergency event.³⁰⁶

Adding to the supply chain issues are the long lead times associated with most electric transmission system material assets, such as transmission towers and special transmission transformers. This issue is due to the inherent size, complexity, and uniqueness of these units, combined with the fact that there are limited U.S. manufacturing facilities.³⁰⁷ This point may be further exacerbated by the fact that the same few equipment suppliers provide critical parts for multiple industries and utilities, which can lead to an acute shortage after a large event.³⁰⁸

³⁰⁶ DOE EPSA, 2015.

³⁰⁷ Meade, 2015.

³⁰⁸ Barrett et al., 2013.

This page intentionally left blank



Global Security Sciences Division

9700 South Cass Avenue, Bldg. 221
Argonne, IL 60439-4854

www.anl.gov



Argonne National Laboratory is a U.S. Department of Energy
laboratory managed by UChicago Argonne, LLC