



Jason McKinney
Editor

ENERGY SCIENCE, ENGINEERING AND TECHNOLOGY

Electricity Delivery and Security

*Federal Oversight,
Activities and Funding*

Novinka

ENERGY SCIENCE, ENGINEERING AND TECHNOLOGY

**ELECTRICITY DELIVERY
AND SECURITY**

**FEDERAL OVERSIGHT, ACTIVITIES
AND FUNDING**

No part of this digital document may be reproduced, stored in a retrieval system or transmitted in any form or by any means. The publisher has taken reasonable care in the preparation of this digital document, but makes no expressed or implied warranty of any kind and assumes no responsibility for any errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of information contained herein. This digital document is sold with the clear understanding that the publisher is not engaged in rendering legal, medical or any other professional services.

ENERGY SCIENCE, ENGINEERING AND TECHNOLOGY

Additional books in this series can be found on Nova's website
under the Series tab.

Additional e-books in this series can be found on Nova's website
under the e-book tab.

ENERGY SCIENCE, ENGINEERING AND TECHNOLOGY

**ELECTRICITY DELIVERY
AND SECURITY
FEDERAL OVERSIGHT, ACTIVITIES
AND FUNDING**

**JASON MCKINNEY
EDITOR**



New York

Copyright © 2017 by Nova Science Publishers, Inc.

All rights reserved. No part of this book may be reproduced, stored in a retrieval system or transmitted in any form or by any means: electronic, electrostatic, magnetic, tape, mechanical photocopying, recording or otherwise without the written permission of the Publisher.

We have partnered with Copyright Clearance Center to make it easy for you to obtain permissions to reuse content from this publication. Simply navigate to this publication's page on Nova's website and locate the "Get Permission" button below the title description. This button is linked directly to the title's permission page on copyright.com. Alternatively, you can visit copyright.com and search by title, ISBN, or ISSN.

For further questions about using the service on copyright.com, please contact:

Copyright Clearance Center

Phone: +1-(978) 750-8400

Fax: +1-(978) 750-4470

E-mail: info@copyright.com.

NOTICE TO THE READER

The Publisher has taken reasonable care in the preparation of this book, but makes no expressed or implied warranty of any kind and assumes no responsibility for any errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of information contained in this book. The Publisher shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the readers' use of, or reliance upon, this material. Any parts of this book based on government reports are so indicated and copyright is claimed for those parts to the extent applicable to compilations of such works.

Independent verification should be sought for any data, advice or recommendations contained in this book. In addition, no responsibility is assumed by the publisher for any injury and/or damage to persons or property arising from any methods, products, instructions, ideas or otherwise contained in this publication.

This publication is designed to provide accurate and authoritative information with regard to the subject matter covered herein. It is sold with the clear understanding that the Publisher is not engaged in rendering legal or any other professional services. If legal or any other expert assistance is required, the services of a competent person should be sought. FROM A DECLARATION OF PARTICIPANTS JOINTLY ADOPTED BY A COMMITTEE OF THE AMERICAN BAR ASSOCIATION AND A COMMITTEE OF PUBLISHERS.

Additional color graphics may be available in the e-book version of this book.

Library of Congress Cataloging-in-Publication Data

ISBN: 978-1-53610-538-4 (eBook)

Published by Nova Science Publishers, Inc. † New York

CONTENTS

Preface		vii
Chapter 1	DOE’s Office of Electricity Delivery and Energy Reliability (OE): A Primer, with Appropriations for FY2016 <i>Fred Sissine</i>	1
Chapter 2	The Smart Grid and Cybersecurity— Regulatory Policy and Issues <i>Richard J. Campbell</i>	31
Chapter 3	Cybersecurity Issues for the Bulk Power System <i>Richard J. Campbell</i>	63
Chapter 4	Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations <i>Paul W. Parfomak</i>	109
Index		159

PREFACE

The federal government first supported a program for energy storage and electric power system technology during the 1970s, before the establishment of the Department of Energy (DOE). In the early days, the program was focused mainly on energy storage—especially to even out the variable power production from wind and solar technologies—but also to support large coal and nuclear power plants. The development of computer capacity and miniaturization has expanded the ability of grid operators to monitor and control electric power flows. The subsequent increase in networking of computerized devices for grid data collection and control advanced the ability of operators to anticipate, avoid, and otherwise mitigate potential power crises, such as blackouts. However, in more recent years, the computerization and networking have become vulnerable to unwanted computer-driven intrusions and disruptions, revealing a new cybersecurity challenge for electric power system technology. The nation’s energy infrastructure is diverse and complex. It includes distributed networks, varied system structures (electricity, oil, and natural gas), an array of operating models (public and private), and different systems in both the physical space and cyberspace. The energy sector consists of thousands of electricity, oil, and natural gas assets¹ that are geographically dispersed and provide for all nationally important systems and networks. Thus, interdependency within the sector and across the nation’s critical infrastructure sectors is significant. Coordinating the security and resilience of energy assets is complicated by the borderless nature of energy and reliance on predominantly privately owned infrastructure. This book examines the federal oversight of electricity delivery and security. It also discusses activities and funding of electricity delivery and security.

Chapter 1 - The nation's energy infrastructure is undergoing a major transformation. New technologies and changes in electricity flows place increasing demands on the electric power grid. These changes include increased use of distributed (mostly renewable energy) resources, Internet-enabled demand response technologies, growing loads from electric vehicle use, continued expansion of natural gas use, and integration of energy storage devices.

The Department of Energy's (DOE's) Office of Electricity Delivery and Energy Reliability (OE) is tasked with the lead role to address those infrastructure issues. OE is also responsible for the physical security and cybersecurity of energy infrastructure. As an illustration, OE reports that, during FY2014, its programs responded to 24 energy-related emergency events, including physical security events, wildfires, severe storms, fuel shortages, and national security events.

Since 2005, the Energy and Water Development (E&W) appropriations bill has funded all DOE programs, including those operated by OE. That office manages five types of research and development (R&D) programs, usually conducted in cost-shared partnership with private sector firms. OE also operates two types of deployment programs, conducted mainly with state and tribal governments. Each OE program office has its own set of goals and objectives.

President Obama has declared grid modernization to be a high priority, stressing its importance to jobs, economic growth, and U.S. manufacturing competitiveness. Further, OE has a key role in supporting the grid integration of renewable energy, which is a focus of the President's Climate Action Plan and is a strategic resource for state responses to the Environmental Protection Agency's proposed Clean Power Plan.

DOE's FY2016 request for OE sought \$270 million, nearly double the FY2015 appropriation of \$147 million. As part of that requested increase, DOE proposed to create a new Transformer Resilience R&D program and a new State Energy Reliability and Assurance grant program. About half of the requested OE increase would have gone to the new grant program. The next largest increases were sought for the Smart Grid and Cybersecurity programs. The FY2016 request also noted that OE plays the central role in two of DOE's broad cross-cutting initiatives: grid modernization and cybersecurity.

For the OE portion of the FY2016 E&W bill (H.R. 2028), the House approved \$160 million and the Senate Appropriations Committee approved \$152 million; but the Administration issued a veto threat. Ultimately, E&W appropriations appeared as Division D of the Consolidated Appropriations Bill

(H.R. 2029). The bill was enacted as P.L. 114-113. The law provided \$206 million for OE. The proposed new grant program was not funded, but funding was provided for the new Transformer Resilience program. Both the Smart Grid and Cybersecurity programs received larger amounts than were requested.

Chapter 2 - Electricity is vital to the commerce and daily functioning of United States. The modernization of the grid to accommodate today's uses is leading to the incorporation of information processing capabilities for power system controls and operations monitoring. The "Smart Grid" is the name given to the evolving electric power network as new information technology systems and capabilities are incorporated. While these new components may add to the ability to control power flows and enhance the efficiency of grid operations, they also potentially increase the susceptibility of the grid to cyber (i.e., computer-related) attack since they are built around microprocessor devices whose basic functions are controlled by software programming. The potential for a major disruption or widespread damage to the nation's power system from a large scale cyberattack has increased focus on the cybersecurity of the Smart Grid.

Federal efforts to enhance the cybersecurity of the electrical grid were emphasized with the recognition of cybersecurity as a critical issue for electric utilities in developing the Smart Grid. The Federal Energy Regulatory Commission (FERC) received primary responsibility for the reliability of the bulk power system from the Energy Policy Act of 2005. FERC subsequently designated the North American Electric Reliability Corporation (NERC) as the "Electric Reliability Organization" (ERO) with the responsibility of establishing and enforcing reliability standards. Compliance with reliability standards for electric utilities thus changed from a voluntary, peer-driven undertaking to a mandatory function. The Energy Independence and Security Act of 2007 (EISA) later added requirements for "a reliable and secure electricity infrastructure" with regard to Smart Grid development. NERC is also responsible for standards for critical infrastructure protection (CIP) which focus on planning and procedures for the physical security of the grid. Self-determination is a key part of the CIP reliability process. Utilities are allowed to self-identify what they see as "critical assets" under NERC regulations. Only "critical cyber assets" (i.e., as essential to the reliable operation of critical assets) are subject to CIP standards. FERC has directed NERC to revise the standards so that some oversight of the identification process for critical cyber assets was provided, but any revision is again subject to stakeholder approval. While reliability standards are mandatory, the ERO

process for developing regulations is somewhat unusual in that the regulations are essentially being established by the entities who are being regulated. This may potentially be a conflict of interest, especially when cost of compliance is a concern, and acceptable standards may conceivably result from the option with the lowest costs. Since utility systems are interconnected in many ways, the system with the least protected network potentially provides the weakest point of access.

Cybersecurity threats represent a constantly moving and increasing target for mitigation activities and mitigation efforts could likewise spiral upward in costs. Recovery of costs may present a major challenge especially to distribution utilities and state commissions charged with overseeing utility costs. EISA only requires states to consider recovery of costs related to Smart Grid systems. FERC has jurisdiction over the bulk power grid, and cannot compel entities involved in distribution to comply with its regulations. Recoverability from a cyber attack on the scale of something which could take down a significant portion of the grid will likely be very difficult, but maintaining a ready inventory of critical spare parts in close proximity to key installations could quicken recovery efforts from some types of attack. The electricity grid is connected to (and largely dependent on) the natural gas pipeline, water supply, and telecommunications systems. Technologies being developed for use by the Smart Grid could also be used by these industries. Consideration could be given to applying similar control system device and system safeguards to these other critical utility systems.

Chapter 3 - In the United States, it is generally taken for granted that the electricity needed to power the U.S. economy is available on demand and will always be available to power our machines and devices. However, in recent years, new threats have materialized as new vulnerabilities have come to light, and a number of major concerns have emerged about the resilience and security of the nation's electric power system. In particular, the cybersecurity of the electricity grid has been a focus of recent efforts to protect the integrity of the electric power system.

The increasing frequency of cyber intrusions on industrial control (IC) systems of critical infrastructure continues to be a concern to the electric power sector. Power production and flows on the nation's electricity grid are controlled remotely by a number of IC technologies. The National Security Agency (NSA) reported that it has seen intrusions into IC systems by entities with the apparent technical capability "to take down control systems that operate U.S. power grids, water systems and other critical infrastructure."

As the grid is modernized and the Smart Grid is deployed, new intelligent technologies utilizing two-way communications and other digital advantages are being optimized by Internet connectivity. Modernization of many IC systems (in particular, the Supervisory Control and Data Acquisition [SCADA] system) also has resulted in connections to the Internet. While these advances will improve the efficiency and performance of the grid, they also will increase its vulnerability to potential cyberattacks. *Black Energy*, *Havex*, and *Sandworm* are all recent examples of malware targeting SCADA systems. New devices (like smart meters) and increasing points of access (such as renewable electricity facilities) introduce new additional areas through which a potential cyberattack may be launched at the grid.

Many cybersecurity actions are reactive to the last threat discovered. While intrusion detection is a priority, some experts say that mitigation of cyber threats requires a focus on attackers, not the attacks. Cybersecurity strategies may shift from figuring out whether a system has been compromised to an understanding of who authored the malicious software and why. Although malware intrusions may not have resulted in a significant disruption of grid operations so far, they still have been possible even with mandatory standards in place. The North American Electric Reliability Corporation's (NERC's) current set of standards, Critical Infrastructure Protection (CIP) Version 5, is moving toward active consideration of bulk electric system security needs rather than just compliance with minimum standards.

Electric utilities emphasize the need for timely information sharing and advocate for liability protection from potential damages resulting from a major cyber event. Some observers argue that it is the responsibility of electric utilities to embrace security as part of their strategic business planning and operations. The National Electric Sector Cybersecurity Organization has identified six failure scenario domains intended to assist utility cybersecurity efforts. These scenarios also illustrate the continuing vulnerability of the grid to potential cyber and physical attacks, or a combination of both.

This report highlights several areas for congressional consideration to improve grid cybersecurity. One issue is whether electric utilities have the resources to make the financial investment and recruit staff to reduce vulnerabilities. Another issue is that NERC CIP standards do not apply to all points of grid connection to the distribution system, and these connections still may represent cyber vulnerabilities. The adequacy of current standards where they do apply is also an issue.

Chapter 4 - The U.S. electric power grid consists of over 200,000 miles of high-voltage transmission lines and hundreds of large transformer substations.

High voltage (HV) transformer units make up less than 3% of U.S. transformers, but they carry 60%-70% of the nation's electricity. Because they serve as vital nodes, HV transformers are critical to the nation's electric grid. HV transformers are also the most vulnerable to damage from malicious acts.

For more than 10 years, the electric utility industry and government agencies have engaged in activities to secure HV transformers from physical attack and to improve recovery in the event of a successful attack. These activities include coordination and information sharing, spare equipment programs, security standards, security exercises, and other measures. There has been some level of physical security investment and an increasing refinement of voluntary security practices across the electric power sector for at least the last 15 years. However, recent grid security exercises, together with a 2013 physical attack on transformers in Metcalf, CA, have changed the way grid security is viewed and have focused congressional interest on the physical security of HV transformers. They have also prompted new grid security efforts by utilities and regulators.

On November 20, 2014, the Federal Energy Regulatory Commission (FERC) approved a new mandatory Physical Security Reliability Standard (CIP-014-1) proposed by the North American Electric Reliability Corporation (NERC). The new standards require certain transmission owners "to address physical security risks and vulnerabilities related to the reliable operation" of the power grid by performing risk assessments to identify their critical facilities, evaluate potential threats and vulnerabilities, and implement security plans to protect against attacks. Legislative proposals would expand federal efforts to prevent or recover from a physical attack on the U.S. grid. These include the Enhanced Grid Security Act of 2015 (S. 1241), the Critical Electric Infrastructure Protection Act (H.R. 2271), the Terrorism Prevention and Critical Infrastructure Protection Act of 2015 (H.R. 85), a House bill to establish a strategic transformer reserve program (H.R. 2244), and the Grid Modernization Act of 2015 (S. 1243).

There is widespread agreement among government agencies, utilities, and manufacturers that HV transformers in the United States are vulnerable to terrorist attack, and that such an attack potentially could have catastrophic consequences. But the most serious, multi-transformer attacks could require acquiring operational information and a certain level of sophistication on the part of potential attackers. Consequently, despite the technical arguments, without more specific information about potential targets and attacker capabilities, the actual risk of a multi-HV transformer attack remains an open question. As the electric power industry and federal agencies continue their

efforts to improve the physical security of critical HV transformer substations, Congress may consider several issues as part of its oversight of the sector: identifying critical transformers, confidentiality of critical transformer information, adequacy of HV transformer protection, quality of federal threat information, recovery from HV transformer attacks, and the overall resiliency of the grid. Maintaining an integrated perspective on prevention, recovery, and resilience may help to promote an effective balance among industry investment, regulatory requirements, and federal oversight.

Chapter 1

**DOE’S OFFICE OF ELECTRICITY DELIVERY
AND ENERGY RELIABILITY (OE): A
PRIMER, WITH APPROPRIATIONS
FOR FY2016***

Fred Sissine

SUMMARY

The nation’s energy infrastructure is undergoing a major transformation. New technologies and changes in electricity flows place increasing demands on the electric power grid. These changes include increased use of distributed (mostly renewable energy) resources, Internet-enabled demand response technologies, growing loads from electric vehicle use, continued expansion of natural gas use, and integration of energy storage devices.

The Department of Energy’s (DOE’s) Office of Electricity Delivery and Energy Reliability (OE) is tasked with the lead role to address those infrastructure issues. OE is also responsible for the physical security and cybersecurity of energy infrastructure. As an illustration, OE reports that, during FY2014, its programs responded to 24 energy-related emergency events, including physical security events, wildfires, severe storms, fuel shortages, and national security events.

* This is an edited, reformatted and augmented version of a Congressional Research Service publication, R44357, dated February 9, 2016.

Since 2005, the Energy and Water Development (E&W) appropriations bill has funded all DOE programs, including those operated by OE. That office manages five types of research and development (R&D) programs, usually conducted in cost-shared partnership with private sector firms. OE also operates two types of deployment programs, conducted mainly with state and tribal governments. Each OE program office has its own set of goals and objectives.

President Obama has declared grid modernization to be a high priority, stressing its importance to jobs, economic growth, and U.S. manufacturing competitiveness. Further, OE has a key role in supporting the grid integration of renewable energy, which is a focus of the President's Climate Action Plan and is a strategic resource for state responses to the Environmental Protection Agency's proposed Clean Power Plan.

DOE's FY2016 request for OE sought \$270 million, nearly double the FY2015 appropriation of \$147 million. As part of that requested increase, DOE proposed to create a new Transformer Resilience R&D program and a new State Energy Reliability and Assurance grant program. About half of the requested OE increase would have gone to the new grant program. The next largest increases were sought for the Smart Grid and Cybersecurity programs. The FY2016 request also noted that OE plays the central role in two of DOE's broad cross-cutting initiatives: grid modernization and cybersecurity.

For the OE portion of the FY2016 E&W bill (H.R. 2028), the House approved \$160 million and the Senate Appropriations Committee approved \$152 million; but the Administration issued a veto threat. Ultimately, E&W appropriations appeared as Division D of the Consolidated Appropriations Bill (H.R. 2029). The bill was enacted as P.L. 114-113. The law provided \$206 million for OE. The proposed new grant program was not funded, but funding was provided for the new Transformer Resilience program. Both the Smart Grid and Cybersecurity programs received larger amounts than were requested.

BACKGROUND

The federal government first supported a program for energy storage and electric power system technology during the 1970s, before the establishment of the Department of Energy (DOE). In the early days, the program was focused mainly on energy storage—especially to even out the variable power production from wind and solar technologies—but also to support large coal and nuclear power plants. The development of computer capacity and

miniaturization has expanded the ability of grid operators to monitor and control electric power flows. The subsequent increase in networking of computerized devices for grid data collection and control advanced the ability of operators to anticipate, avoid, and otherwise mitigate potential power crises, such as blackouts. However, in more recent years, the computerization and networking have become vulnerable to unwanted computer-driven intrusions and disruptions, revealing a new cybersecurity challenge for electric power system technology.

The nation's energy infrastructure is diverse and complex. It includes distributed networks, varied system structures (electricity, oil, and natural gas), an array of operating models (public and private), and different systems in both the physical space and cyberspace. The energy sector consists of thousands of electricity, oil, and natural gas assets¹ that are geographically dispersed and provide for all nationally important systems and networks. Thus, interdependency within the sector and across the nation's critical infrastructure sectors is significant. Coordinating the security and resilience of energy assets is complicated by the borderless nature of energy and reliance on predominantly privately owned infrastructure.

Key challenges and opportunities facing the electric power industry include a changing power generation mix, replacing aging infrastructure (transmission, storage, distribution, and generation); updating communication networks (e.g., analog to digital); accommodating new end-use technologies such as distributed resources; planning for increased interdependencies of natural gas, water, and electricity systems; and devising business models that manage these challenges in providing reliable and affordable electricity service. These activities must be balanced against the need for cost control, physical security, cybersecurity, improved reliability and resiliency, and flexibility to deal with market uncertainties and a changing climate. Additional opportunities arise due to increasing natural gas production from shale and decreasing costs for information technologies that allow grid operators to better monitor and control the grid and that enable customers to better manage power use.

ORGANIZATION AND STRATEGY

Mission

The DOE Office of Electricity Delivery and Energy Reliability (OE) is charged with a mission to support more economically competitive, environmentally responsible, secure, and resilient U.S. energy infrastructure.² To achieve that mission, OE supports electric grid modernization and resiliency through research and development (R&D), demonstration projects, partnerships, facilitation, modeling and analytics, and emergency preparedness and response. It is the federal government's lead entity for energy sector-specific responses to energy security emergencies— whether caused by physical infrastructure problems or by cybersecurity issues.

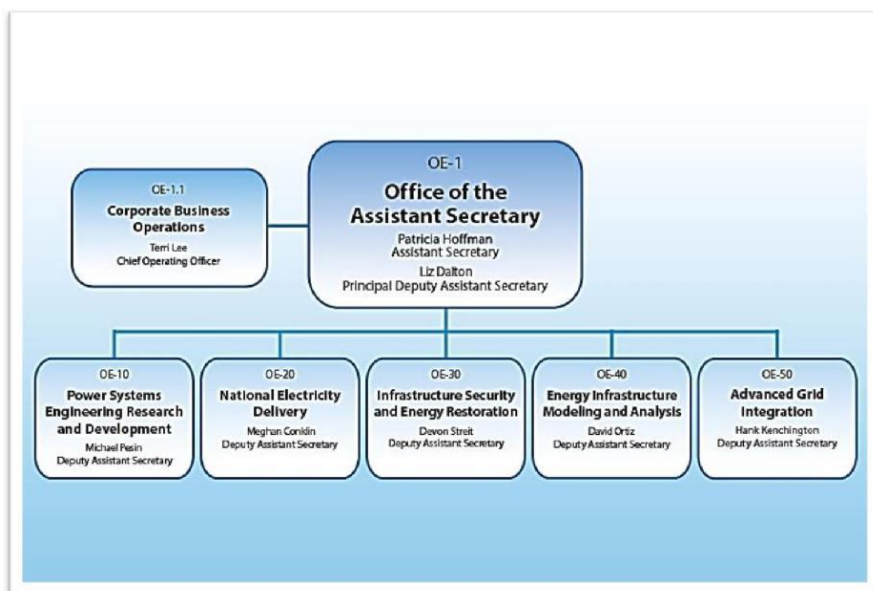
OE leads DOE's efforts to strengthen, transform, and improve our energy infrastructure so that consumers have access to reliable, secure, and clean sources of energy. To accomplish this mission, the Office works with private industry and federal, state, local, and tribal governments on a variety of initiatives to modernize the electric grid. Grid modernization is critical to addressing aging infrastructure, achieving public policy objectives, sustaining economic growth, supporting environmental stewardship, and mitigating risks to secure the nation. The goal for the future grid is to support economic growth and energy innovation through delivery of reliable, affordable, and clean electricity to consumers where, when, and how they want it.³

Organizational Structure

In 2007, DOE established an independent Assistant Secretary for OE and, thereby, elevated the office to an administrative status equal to that for the major energy technologies (nuclear, fossil, renewables).⁴ OE currently has five deputy assistant secretaries, each of whom reports to the Assistant Secretary. This structure is displayed in *Figure 1*, below.

Strategy and Planning

OE's mission is guided mainly by two key DOE planning documents: the *Quadrennial Technology Review* and the *Grid Modernization Multi-Year Program Plan*.



Source: DOE, Office of Electricity Delivery and Energy Reliability, Our Organization, <http://energy.gov/oe/aboutus/our-organization>.

Figure 1. OE Organizational Structure. (As of January 2016)

DOE Quadrennial Technology Review

DOE's second (2015) Quadrennial Technology Review (QTR) outlined key elements of the department's strategy for grid modernization. The report concluded that

Fundamental changes in both supply and demand technologies are placing new requirements on the electric power system. On the supply side, there is a diversification of resources as aging, low-efficiency capacity is replaced by a mix of central stations and distributed generation, powered by a mix of fossil and renewable resources. On the demand side, diversification includes a rapidly growing use of distributed generation and interactive control systems in buildings, industrial equipment, and consumer goods. Accompanying these changes is a convergence of digital communications and control systems ("smart grid" technologies) to improve performance and engage consumers. Additionally, grid operations are moving from directing systems with a handful of control points at central stations to ones with potentially millions of highly interactive distributed control points. These trends create new technical requirements for a grid that is more flexible and

agile, with the ability to dynamically optimize grid operations in near-instant time frames.”⁵

Further, from the cross-cutting programs viewpoint, the report stressed the R&D aspects of grid modernization:

The electric grid is transitioning from a centrally-controlled, predictable system with one-way power flows in distribution to a much more distributed, stochastic, and dynamic system with bi-directional flows in distribution. Growth in the deployment of variable generation, electronic converters, and digital communications and control technologies is impacting core characteristics of the electricity system. Grid-related technologies need to evolve with the changing supply and end-use technologies landscape. Simultaneously, the RDD&D [research, development, demonstration, and deployment] associated with technologies that connect to the grid (e.g., renewable power supplies, efficient motor controllers, and smart loads) should consider the evolving interface with the grid. If electricity displaces petroleum and natural gas in electric vehicles and heating applications, respectively, the grid may serve an even more central role in the future energy system. The RDD&D opportunities identified for this rapidly evolving sector include planning models, operational tools, transmission components, distribution hardware, control systems, electricity storage and cybersecurity. These opportunities need to be developed in anticipation of an agile, flexible, and resilient electric power system to enable effective integration of variable supplies and participatory demand.⁶

Grid Modernization Multi-Year Program Plan (MYPP)

DOE’s 2015 *Grid Modernization MYPP* describes its vision for “a future electric grid that provides a critical platform for U.S. prosperity, competitiveness, and innovation by delivering reliable, affordable, and clean electricity to consumers where they want it, when they want it, how they want it.”⁷ To help achieve this vision, DOE targets three key national targets:

- A 10% reduction in the economic costs of power outages by 2025.
- A 33% decrease in the cost of reserve margins while maintaining reliability by 2025.
- A 50% decrease in the net integration costs of distributed energy resources by 2025.⁸

The initiative will assess its progress not only by looking at RD&D efforts in individual technical areas but also by looking at three integrated demonstrations, referred to in the MYPP as DOE major technical achievements. They are:

1. *A transmission and distribution system operating reliably on a lean reserve margin.* Full power system visibility will be provided by real-time sensor networks enabling new approaches to system design, control, operations, protection, and optimization. There will be an integrated effort to demonstrate the delivery of reliable and affordable grid services with a substantially reduced amount of system reserve capacity.
2. *Resilient distribution feeders with high percentages of low-carbon distributed energy resources (50%).* This will be achieved through advances in real-time system monitoring, for high penetration of clean, distributed generation, and the proliferation of smart consumer end-use devices. There will also be new approaches to distributed control, engagement with bulk system reliability management, and coordination across local intelligent assets, including multiple microgrids, over a range of feeder innovations that meet both changing consumer expectations and traditional demand for reliability, resilience, and affordability.
3. *An advanced modern grid planning and analytics platform.* This will be a platform of integrated high performance tools that couple transmission, distribution and communications tools. These tools will have the capacity to reflect uncertainty, and substantially increase the speed and productivity of tools that enable stakeholders to achieve timely evaluation of future grid alternatives. This platform will be integrated with vendor products and leveraged into ongoing technical assistance with states and regions to substantially improve planning and regulatory assessments of the modern grid.⁹

The MYPP states that multiple demonstrations will be conducted across various regions of the country to underpin these “major technical achievements.” Those major grid modernization achievements will be supported by six specific technical areas: (1) Devices and Integrated Systems Testing, (2) Sensing and Measurements, (3) System Operations, Power Flow, and Control, (4) Design and Planning Tools, (5) Security and Resilience, and (6) Institutional Support.¹⁰

Administration Perspective and Goals

OE also plays a critical role in implementation of the President's Climate Action Plan to mitigate the risks and enhance resilience against threats posed by climate change. The FY2016 OE request aimed to support the Administration's "all-of-the-above" energy strategy and emphasized priorities that increase electric grid resilience—through managing risks, increasing system flexibility and robustness, increasing visualization and situational awareness, and deploying advanced control capabilities.

PROGRAM FUNDING HISTORY

Spending History in Context

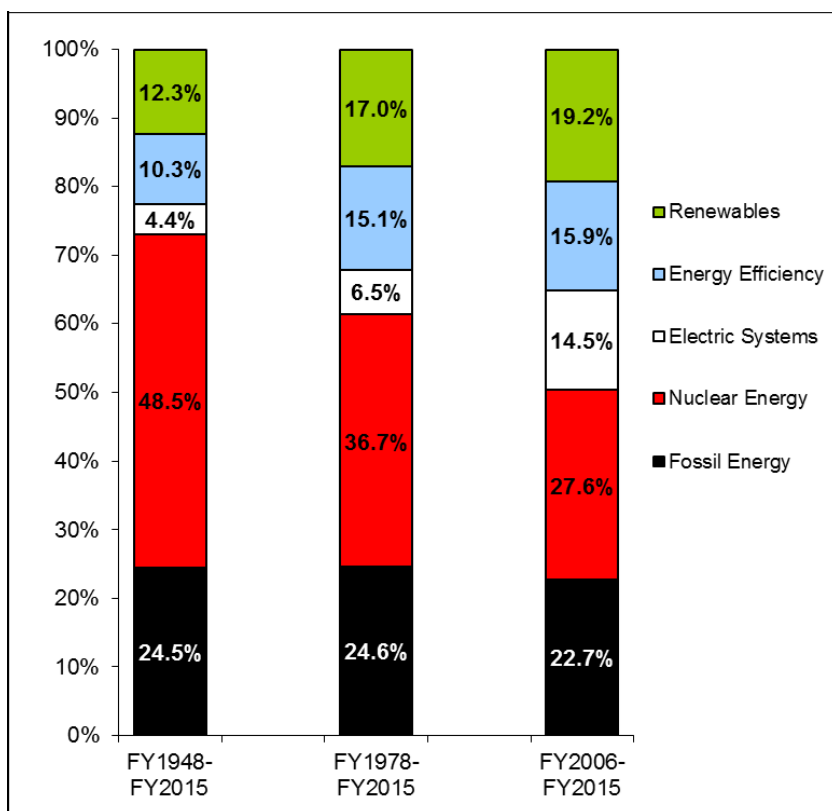
Historically, electric systems technology development programs have supported all four major types (nuclear, fossil, renewable, efficiency) of energy technology. For most of DOE's funding history, OE programs received a relatively small portion of funding, compared to the portion provided for the energy technology programs.¹¹

Recovery Act Funding

However, the OE program received a major one-time boost in funding—\$4.5 billion—from the American Recovery and Reinvestment Act of 2009 (Recovery Act, P.L. 111-5).¹² The funding was targeted for "grid modernization." Thus, much of it was used to provide grants to the electric utility industry to deploy smart grid technologies to modernize the electric grid. As a part of these programs, independent system operators (ISOs), regional transmission organizations (RTOs), and electric utilities installed about 1,100 synchrophasors¹³ and other related technologies in their electric power transmission systems.¹⁴ That deployment of synchrophasors, however, covered only a small portion of the total national grid.

Funding Comparison with Energy Technologies

Figure 2 provides a condensed visual summary of the relative portion of funding for electric systems in three different historical time periods.



Source: DOE Budget Authority History Table by Appropriation, May 2007; DOE Congressional Budget Requests (several years); DOE (Pacific Northwest Laboratory), An Analysis of Federal Incentives Used to Stimulate Energy Production, 1980; DOE Conservation and Renewable Energy Base Table, February 1990. Deflator Source: The Budget for Fiscal Year 2016. Historical Tables, Table 10.1.

Notes: Column to far left shows shares for the period FY1948-FY2015; middle column shows shares for period from FY1978-FY2015; and far right column shows shares for period from FY2006-FY2015.

Figure 2. DOE Energy Technology Share of Funding, Comparison over Three Periods (Chart taken from CRS Report RS22858)

Recent Appropriations History

Since 2005, the Energy and Water Development (E&W) appropriations bill¹⁵ has funded all DOE programs, including those operated by OE.¹⁶ The

office mainly conducts R&D, which is often performed in partnership with industry. OE administers a wide range of R&D programs, each with its own set of goals and objectives.

Since FY2011, DOE has requested sizeable increases in spending each year, but Congress did not significantly boost spending until FY2016. *Table 1*, below, shows the recent pattern of OE requests and final appropriation levels.

**Table 1. OE Requests and Final Appropriations,
FY2011–FY2016
(\$ millions, current)**

Fiscal Year	Request	Final Appropriation
FY2011	\$186	\$141
FY2012	\$238	\$139
FY2013	\$143	\$132
FY2014	\$169	\$147
FY2015	\$180	\$147
FY2016	\$270	\$206

Source: DOE Budget Requests, FY2011 through FY2016; and personal communication with Yulia Korzh, OE, February 8, 2016.

Notes: The FY2016 OE figure was provided in Division D of the Consolidated Appropriations Act, FY2016.

FY2016 HIGHLIGHTS

Summary

DOE presented its FY2016 budget request on February 2, 2015.¹⁷ The request for OE was \$270 million, which would have nearly doubled the FY2015 level.¹⁸ As part of that requested increase, DOE proposed to create a new Transformer Resilience and Advanced Components R&D program and a new State Energy Reliability and Assurance grant program. About half of the requested OE increase would have gone to the new grant program. The next largest increases were sought for the Smart Grid and Cybersecurity programs.

The House Committee on Appropriations reported the Energy and Water Development (E&W) Appropriations Bill, 2016 (H.R. 2028) with a recommendation of \$187.5 million for OE.¹⁹ The \$187.5 million figure for OE was adopted in House floor action.²⁰ Subsequently, the Senate Committee on Appropriations recommended \$152.3 million.²¹ The congressionally

recommended overall amount for DOE drew a veto threat from the Administration mainly for reasons unrelated to OE funding. Subsequently, the E&W bill was incorporated as Division D of the Consolidated Appropriations Act, FY2016 (H.R. 2029). The final enacted version of H.R. 2029 (P.L. 114-113, Division D) provided \$206 million for OE.²²

Congressional Action

After the Administration issued its FY2016 budget request, Congress held a number of DOE oversight and appropriations hearings. As noted above, further actions were taken in the House and Senate on DOE funding recommendations in the E&W bill, H.R. 2028. Late in the first session, after lengthy negotiations, the E&W bill was incorporated into H.R. 2029. The various steps of the congressional process for the FY2016 E&W appropriations are outlined in *Table 2*.

**Table 2. OE FY2016 Appropriations Chronology
(Highlights of Committee and Floor Action,
with Administration responses)**

Date	Action
February 2, 2015	DOE issues FY2016 budget request.
February 11, 2015	House Energy and Commerce Committee's Subcommittee on Energy and Power held a hearing on the DOE request.
February 12, 2015	Senate Committee on Energy and Natural Resources (SENRR) held a hearing on the DOE request.
February 26, 2015	House Appropriations Committee's Subcommittee on Energy and Water Appropriations held a hearing on the DOE request.
March 25, 2015	Senate Appropriations Committee's Subcommittee on Energy and Water Appropriations held a hearing on the DOE request.
April 13, 2015	House Appropriations Committee's Subcommittee on Energy and Water Appropriations released a draft report with recommended funding for FY2016 E&W appropriations bill.
April 15, 2015	House Appropriations Committee's Subcommittee on Energy and Water Appropriations held a subcommittee markup.
April 21, 2015	House Appropriations Committee issued draft report on FY2016 E&W appropriations bill with recommended funding for FY2016 E&W appropriations bill.

Table 2. (Continued)

Date	Action
April 21, 2015	Office of Management and Budget (OMB) issued a letter to the House Appropriations Committee that expressed the Administration's concerns with the draft E&W appropriations bill.
April 22, 2015	House Appropriations Committee held a full committee markup. Several amendments were adopted, none of which affected the provisions for OE.
April 24, 2015	House Appropriations Committee issued the E&W appropriations bill (H.R. 2028) and final report (H.Rept. 114-91) with recommended funding for FY2016 E&W appropriations.
April 28, 2015	OMB issued a Statement of Administration Policy that strongly opposed House passage of H.R. 2028.
May 1, 2015	House approved H.R. 2028, without amendments to the committee recommendations for OE.
May 21, 2015	Senate Appropriations Committee reported (S.Rept. 114-54) its recommendations for H.R. 2028.
December 17, 2015	House approved H.R. 2029, Consolidated Appropriations Act, 2016. A modified version of the E&W appropriations bill (H.R. 2028) was included as Division D. The explanatory statement on H.R. 2029 was printed in Congressional Record.
December 17, 2015	Senate approved H.R. 2029.
December 18, 2015	President signed H.R. 2029 into law as P.L. 114-113. The E&W bill was incorporated as Division D.

Source: Multiple sources were used.

Funding Increases

This section presents the key OE program funding increases enacted and describes some highlights for each of those programs.

Increases Ranked by Program

Several programs received a significant funding increase for FY2016. *Table 3* shows all program increases in dollar amounts and percentages, relative to FY2015.

**Table 3. OE FY2016 Program Increases, in Rank Order
(\$ millions, FY2016-FY2015 difference)**

Program	Increase	Percent Increase
Smart Grid R&D	\$19.6	127%
Cybersecurity (CEDS)	\$16.0	35%
Energy Storage	\$8.5	71%
Transformer Resilience (TRAC)	\$5.0	—
Clean Energy Transmission and Reliability (CETR)	\$4.7	14%
Infrastructure Security and Energy Restoration (ISER)	\$3.0	50%
National Electricity Delivery (NED)	\$1.5	25%

Source: Congressional Record, Explanatory Statement on Consolidated Appropriations Act, 2016, December 17, 2015, pp. H10108-H10109, <https://www.congress.gov/crec/2015/12/17/CREC-2015-12-17-bk2.pdf>.

Notes: Transformer Resilience is a new program for FY2016.

Highlights of Key Program Increases

Table 3 shows that the largest OE increases are for smart grid and cybersecurity.²³ A discussion of the planned FY2016 activities in these two areas follows.

Smart Grid

Congress provided \$5 million more than the nearly \$15 million increase sought in the DOE request. The *Explanatory Statement for H.R. 2029* (P.L. 114-113) was silent on the focus of the approved \$5 million increase over the DOE request.

The DOE request stated that the “endpoint target” of the smart grid program is “achievement of a self-healing and resilient distribution grid, with integration of networked microgrids and market-based control signals operating under the ADMS [advanced distribution management system] that allows for widespread deployment of distributed renewable and clean energy resources and demand response by 2030.”²⁴ Specifically, the DOE-requested portion of the increase aims to launch two new efforts: ADMS technologies and market-based signal controls (MBCS).

- ADMS software will support distribution management and the integration of large amounts of renewable energy.²⁵
- MBCS will employ simulation and test cases to improve operational flexibility for increased use of customer and third-party assets

(including end-use devices, batteries, distributed generation, solar power, and electric vehicle chargers).²⁶

Cybersecurity

Congress provided \$10 million more than the DOE requested increase of \$6 million. The *Explanatory Statement for H.R. 2029* (P.L. 114-113) was silent on the focus of the approved increase over the DOE requested amount.

The DOE request stressed “the critical need to accelerate and expand efforts to strengthen the energy infrastructure against cyber threats.”²⁷ Specifically, the DOE-requested portion of the increase aimed to establish a “virtual energy sector advanced digital forensics analysis platform.” In simpler terms, this project will apply virtual reality visualization technologies to help utilities distinguish between a normal system failure and malicious activity and to help them mitigate any malicious activity.²⁸

Cross-Cutting Initiatives

The FY2016 request also sought to continue crosscutting programs that coordinate across the department and seek to tap DOE’s full capability to effectively and efficiently address national energy, environmental, and national security challenges. OE serves as the central part of the Grid Modernization and Cybersecurity crosscut programs.

FY2016 FUNDING TABLE

OE operates seven program offices²⁹ and one administrative office. Each program office has its own set of goals and funding needs. *Table 4* shows the funding breakdown by program office.

PROGRAM GOALS AND ACTIVITIES

For FY2016, the OE request proposed to create one new R&D program (Transformer Resilience and Advanced Components), which was funded,³⁰ and a new grant program (State Energy Reliability and Assurance), which was

not funded. For each of the existing and proposed programs, this section describes goals, objectives, and funding.

Table 4. Electricity Delivery and Energy Reliability (OE) Appropriations (\$ millions)

Program	FY2013 Approp.	FY2014 Approp.	FY2015 Approp.	FY2016 Approp.	FY2016- FY2015	Percent Change
Clean Energy Transmission and Reliability (CETR)	24.1	32.4	34.3	39.0	4.7	13.7%
Smart Grid R&D	20.6	14.6	15.4	35.0	19.6	127.0%
Cybersecurity for Energy Delivery Systems (CEDS)	30.1	43.5	46.0	62.0	16.0	34.8%
Energy Storage	18.9	15.2	12.0	20.5	8.5	70.8%
Transformer Resilience and Advanced Components (TRAC)	—	—	—	5.0	5.0	—
National Electricity Delivery(NED)	6.6	6.0	6.0	7.5	1.5	25.0%
Infrastructure Security and Energy Restoration (ISER)	6.1	8.0	6.0	9.0	3.0	50.0%
Program Direction	25.6	27.6	27.6	28.0	0.4	1.4%
Total OE Appropriation	132.0	147.2	147.3	206.0	58.7	39.9%

Source: DOE Budget Requests for FY2015 and FY2016, vol. 3; and P.L. 114-113, Division D. Personal communication with Yulia Korzh, OE, February 8, 2016.

Clean Energy Transmission and Reliability (CETR)³¹

The electricity system depends upon the inherent stability of a network of traditional power plants to balance electric power supply and demand. When disruptions occur, power grid operators are usually able to take actions to maintain system stability. However, the basic structure of the system is changing. In particular, the rising levels of wind and solar power generation create resource uncertainty and electric current instability. Both conditions pose a challenge to system stability. Also, a widening range of loads (e.g., backup for rooftop solar) are becoming active participants in the electricity system, which adds more complexity to system models and operations.³²

The electricity system must provide key services even during disruptions. A growing number of extreme weather-related events highlight the urgent need for reliable and robust monitoring, modeling, and analytical tools to

support both industry operations and governmental emergency response efforts.

The CETR program aims to improve energy system decisionmaking by fostering the development of system measurement, modeling, and risk analysis. The program is designed to lay the foundation for a modern grid and ensure that elements of risk and uncertainty are properly addressed in decisions about investments to improve energy infrastructure. CETR activities are organized into three R&D subprograms: Transmission Reliability, Advanced Modeling Grid Research, and Energy Systems Risk and Predictive Capability.

Transmission Reliability Program

Existing electric transmission lines were designed to carry electric power from major power plants to urban and industrial load centers. The grid was originally designed mostly for this purpose—not for the market-driven flows of power that it currently serves. Usually mounted on tall metal towers, these lines operate at high voltage and carry high levels of electric current. Competition and market forces are causing the volume of power transactions to grow rapidly. Also, the structure of power generation is changing—due to coal plant retirements, increased use of natural gas-fired generators, and integration of large wind farms. This decentralization of the power generation mix can affect power quality and causes the grid to be used in ways for which it was not originally designed.

Special electric power sensors, known as synchrophasors,³³ were designed to monitor (measure) electric power flow with high precision and, thus, can reveal much about the health of power systems. The Transmission Reliability program supports the development of cyber-secure grid management applications that employ synchrophasors to enhance the flexibility, reliability, and resilience of the national power system. Spurred by the Northeast blackout of 2003, DOE joined with electric utilities and the North American Electric Reliability Council (NERC) to install synchrophasors throughout the grid. The Recovery Act of 2009 (P.L. 111-5) provided \$4.5 billion for the smart grid and grid modernization provisions in EISA (Title 13).³⁴ A large portion of those funds were used to accelerate the rate of synchrophasor deployment. As the network of these devices expands, the richer³⁵ data pattern and yield enables the advancement of grid operator tools to detect, track, and analyze grid dynamics and to provide real-time visual monitoring of system conditions.³⁶ OE expects these advances to lead to automated system controls and to reduce the spread and duration of system outages by 2020.

In FY2016, OE expects to complete “production-grade” grid operator software applications that will be purchased by utilities.³⁷ The expanded software applications would be applied to the use of microgrids, energy storage, distributed generation, and electric vehicle charging.

Advanced Modeling Grid Research Program

This program conducts research on computer models that underpin energy management systems used by grid operators to plan, monitor, and control the electric system. The goal is to enhance reliability and enable advanced problem mitigation and recovery strategies. Objectives include improved grid resilience to events that otherwise rapidly drive network failures and blackouts; developing predictive capabilities for system anomalies and uncertainties; and integrating models to improve operational planning and enable dynamic reconfiguration of electric system elements to achieve technical and economic objectives. R&D activities focus on data management and the development of computer models and simulations.

Energy Systems Risk and Predictive Capability (ESRPC) Program

The need for national capabilities to assess near- and long-term risks to energy infrastructures was illustrated by the massive impacts of Superstorm Sandy (2012), the major hurricanes in 2008 (Gustav and Ike) and in 2005 (Katrina and Rita), and the 2013-2015 western drought and accompanying wildfires. ESRPC's goal is to advance national capability for risk-informed decisionmaking for energy systems. Potential near-term actions include developing strategies to reduce the risk of system interruptions due to extreme weather. Longer-term actions include identifying a portfolio of energy system improvements that could reduce the system-wide risks from weather events.

For FY2016, ESRPC will focus on developing analytical tools that estimate seasonal and regional extreme weather risks to energy systems that cover large geographic areas. ESRPC's research covers three types of analytic products and predictive models for system planning: (1) real-time information on extent of disruption and likely near- and long-term effects, (2) long-range (five- to eight-year timeframe) risk guidance for investment in national energy infrastructure (e.g., effect of sea level rise on infrastructure in cities), and (3) guidance for nontraditional sources of manmade risk, such as supply chain disruptions.

Smart Grid R&D³⁸

This program develops technologies, tools, and techniques to modernize the distribution portion of the electric delivery system—power lines, transformers, and other infrastructure—that takes power from the high-voltage transmission system and delivers it to individual businesses and homes.³⁹ Program goals aim to accommodate rising amounts of customer-owned generation equipment (e.g., solar photovoltaics, PV), support the shift to electric vehicles (EVs), improve resilience to extreme weather events, reduce outages, and enable greater customer control over power use and quality while maintaining electric power affordability.

Information and communication technologies play a key role in Smart Grid goals to address technical challenges such as rising demand and supply variability, two-way power flow, data management and security, interoperability between new and legacy technologies, and the increasing linkages of distribution and transmission operations.

Microgrids

There is a major focus on microgrids, which are localized power grids that can disconnect from the traditional grid to operate independently.⁴⁰ Because most power outages occur at the distribution level, microgrid developments can help mitigate grid disturbances and strengthen grid resilience. OE's microgrid program goals are to develop commercial scale microgrid systems (with a capacity less than 10 megawatts)⁴¹ that are capable of reducing outage time of required loads by more than 98%. This would be accomplished at a cost comparable to non-integrated baseline solutions, while reducing emissions by 20% and improving system energy efficiencies by 20% by 2020.⁴²

Advanced Distribution Management Systems (ADMS)

This program promotes higher performing grids by integrating new assets and information streams with ADMS. An OE report describes these systems:

ADMS is a software platform that integrates numerous utility systems and provides automated outage restoration and optimization of distribution grid performance. ADMS functions can include automated fault location, isolation, and service restoration (FLISR); conservation voltage reduction; peak demand management; and volt/volt-ampere reactive (volt/VAR) optimization.⁴³ In effect, an ADMS transitions

utilities from paperwork, manual processes, and siloed [separated] software systems to systems with real-time and near-real-time data, automated processes, and integrated systems.⁴⁴

The report on ADMS notes further that existing mechanisms for the diagnosis of end-of-the-line power problems have yet to employ modern computer capabilities:

Considering that this is an era in which smart phones and Google Maps are ubiquitous, it may come as a surprise that utilities have very little visibility into their distribution systems. Most systems still rely on breakers to disconnect the lines in the event of a fault, customers to call in to report an outage, and line crews to find the affected circuit and restore power.⁴⁵

DOE observes that ADMS is a fledgling industry that lacks mature, field-proven vendor products. However, DOE's technology program is working with vendors to help fill that gap. ADMS integration into existing utility operating systems is difficult. Those systems were traditionally custom-built, and evolved with technologies over the course of several decades. Integrating new systems with old—or getting them to “talk” to each other—is complicated and requires an information technology foundation that can support each component of an ADMS.⁴⁶

In FY2016, the program aims to enhance operational visibility and system asset control. It will start the development of an open source ADMS platform that supports the full range of distribution management applications (such as fault location, service restoration, and operational optimization). Also, the program will begin to develop data analytics for large volumes of grid data needed to validate distribution grid operations.

Market-Based Control Strategies (MBCS)

Smart Grid investments will also explore market-based controls in FY2016. The process of coupling market-based control signals with electric distribution operations is generally known as transactive energy. Transactive energy refers to the use of a combination of economic (resource bidding) and physical control techniques to improve grid reliability and efficiency. Regarding the economic aspect, a transactive energy system may lead to collection of data from more nodes (access points on the grid) and, thus, yield finer-grained levels of real-time pricing for each data point.⁴⁷ Also, by

coordinating the activity of the growing number of distributed energy resources, transactive energy systems can help maintain power system reliability and security while increasing efficiency.⁴⁸ Development of the MBCS process is intended to create value to both utilities and customers. This new control paradigm is to enable utilities to balance supply and demand at all levels of the grid, by actively seeking participation of customer-owned and third-party assets in grid services through transparent, competitive forces of demand and supply.⁴⁹ The prices or incentives offered by market forces will engage the self-interest of customers and other third parties, and will also serve as a control signal to coordinate operation of their assets with the power grid. Hence, transactive energy will result in greatly increased flexibility needed for maintaining reliability in a low-carbon future, while allowing customers to fully participate in grid operations.

For FY2016, the program aims to develop simulation tools and to apply validating tools to initial test cases that were funded by the Recovery Act. Transactive approaches will be evaluated to refine controllability, stability limits, and efficacy of operating distributed assets (end-use devices, distributed generation, batteries, PV solar systems, inverters, EV chargers, etc.) and networked communication systems.

Cybersecurity for Energy Delivery Systems (CEDS)⁵⁰

Reliable and resilient energy infrastructure is essential to our economy, health and safety, and national security. OE's mission to modernize the electric grid cannot be achieved without the research, development, and integration of secure energy delivery control systems. The energy sector—including electricity, oil, and natural gas—has experienced a dramatic increase in cyber probes,⁵¹ data exfiltration,⁵² and malware⁵³ development for potential attacks. The growing seriousness of these intrusions marks an era of state actor level threats to the nation. The dynamic cyber threat landscape, continuous advances in energy delivery system technologies, and the use of legacy devices in ways not previously envisioned underscore the importance of this continuous transition.

The Cybersecurity (CEDS) program aims to strengthen the energy infrastructure against current and future cyber threats. The strategic framework for DOE's role is shaped mainly by Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*.⁵⁴ The directive calls on the sector-

specific agencies (SSAs) to serve as a day-to-day federal interface for the dynamic prioritization and coordination of various sector-specific activities. As the energy SSA, DOE has the mission, history, and expertise to work with industry to mitigate the risk of cyberattacks on the energy system. To fulfill this responsibility, DOE collaborates with vendors, utility owners, and operators of the electricity and oil and natural gas sectors to strengthen the cybersecurity of critical energy infrastructure.

OE has the lead role in addressing this DOE responsibility. To meet this requirement the CEDS program conducts cyber risk and incident management activities with four key objectives: (1) accelerate information sharing to enhance situational awareness; (2) expand implementation of the Cybersecurity Capability Maturity Models and Risk Management Process, (3) conduct technology R&D to improve energy reliability and resilience, and (4) exercise and refine the energy sector's cyber incident response capabilities.

Energy Storage⁵⁵

The Storage program is designed to develop and demonstrate new and advanced energy storage technologies (e.g., batteries, pumped hydro, flywheels) that will enable the stability, resiliency, and reliability of the future electric utility grid. The program also aims to support increased use of variable renewable energy resources such as wind and solar power generation. The Storage program addresses four challenges identified in the 2013 DOE strategic plan for *Grid Energy Storage*:⁵⁶ cost-competitive energy storage technology, validated reliability and safety, equitable regulatory environment, and industry acceptance.

The implementation of grid-scale energy storage projects throughout the country is accelerating. Microgrids involving storage are being installed by the military for energy security and by states, including New Jersey and Massachusetts, for emergency preparedness. However, storage technology still needs to make substantial improvements in safety, cycle life, energy density, and cost before becoming fully competitive. R&D activities focus on lowering cost while improving the value, performance, safety, and reliability of stationary energy storage technologies for utility-scale applications.

Transformer Resilience and Advanced Components (TRAC)⁵⁷

DOE requested a new funding line to establish this new program in FY2016. The focus is on shielding electric system transformers⁵⁸ from a variety of sources that could inflict damage by creating unwanted electric currents. Larger-scale electric utility transformers are vulnerable to certain conditions that can cause a spike in current or voltage.⁵⁹ If not protected from such threats, damage to a transformer creates vulnerabilities for other electric system equipment. The proposed program's activities would expand upon initial work funded previously under OE's Infrastructure Security and Emergency Response (ISER) program.

Transformers and utility substation equipment are often exposed to the elements and are vulnerable to natural and man-made threats. To ensure a reliable and resilient power system, grid components need to be designed and built to withstand the impact of lightning strikes, extreme weather, sun-driven "space weather,"⁶⁰ electrical disturbances, accidents, equipment failures, and attacks (physical or cyber). Currently, 70% of large power transformers (LPTs) are aged 25 years or more, 60% of circuit breakers are aged 30 years or more, and 70% of transmission lines are aged 25 years or more. The advanced age of these components degrades their ability to withstand physical stresses and may result in higher failure rates. Failure of key components can lead to widespread outages and long recovery times.⁶¹

The TRAC program supports grid modernization and resilience by addressing the unique challenges facing transformers and other key components that transport power from generation sites to demand sites. As the hardware of the electric power system evolves to improve resilience and accommodate clean energy sources, R&D and testing is needed to understand the physical impact this evolution has on transformers and other vital grid components and to adapt these components with new technologies.

The program will analyze the impact of geomagnetically-induced⁶² ground currents (GIC) on the power grid and support power electronics development. The TRAC program aims to advance the understanding of the risks and impacts of geomagnetic disturbances (GMD) and electromagnetic pulses (EMP) on large power transformers (LPTs) and other grid components.⁶³

LPTs are the most critical pieces of equipment in the grid. Induced currents from GMD/EMP can overload LPTs, damaging internal components and increasing failure rates. The nature of the vulnerability of different types of transformers to GMD/EMP as well as the predictability of GMD phenomena is not well understood.

Additionally, increased use of distributed generation will introduce new challenges with reversed power flows, increased harmonics,⁶⁴ and larger fault currents that can impact transformers and other grid components. The program will be conducted in close cooperation with equipment manufacturers and electricity asset owners and operators.⁶⁵

National Electricity Delivery (NED)⁶⁶

Upon request, this program provides technical and policy expertise to states, regions, and tribes to help develop and implement reliable and affordable electricity infrastructure. NED also authorizes the import and export of electricity, issues permits for cross-border transmission lines, and coordinates federal transmission permitting on federal lands.

The NED program helps state, regional, local, and tribal entities to develop, refine, and improve their electric power programs, policies, and laws. Also, the program helps these entities develop and implement reliable and affordable electricity infrastructure—including generation, transmission, storage, distribution, and demand-side electricity resources. Through this work, OE aims to strengthen these individual systems, which in turn will strengthen the entire electricity infrastructure.

At the federal and international level, NED leads governmental actions in authorizing electricity exports and permitting transmission infrastructure construction across international borders. Also, in accordance with the Federal Power Act, NED conducts a triennial national transmission congestion study,⁶⁷ and helps coordinate transmission permitting on federal lands.

Infrastructure Security and Energy Restoration (ISER)⁶⁸

The ISER program leads national efforts to enhance the reliability, survivability, and resiliency of all national energy infrastructure, including that for electricity, petroleum, and natural gas. The program aims to mitigate consumer energy disruptions and—when energy emergencies occur—to drive an efficient restoration process. ISER conducts activities in cooperation with public and private sector stakeholders, including asset owners and operators. Its key partners include industry and state governments.

ISER activities are grouped under three main areas: (1) executing effective emergency preparedness, response, and restoration operations; (2) providing

reliable energy infrastructure tactical analysis (event analysis) and situational awareness to all stakeholders; and (3) encouraging a risk-based approach to energy system assurance.

The program provides long-term strategic actions to help secure the national energy supply against a variety of challenges. Those challenges include more frequent, stronger, and more destructive weather events; increasing incidents of physical attacks; potential accidents as a result of aging infrastructure or human error; high-impact, low frequency (HILF) threats such as a catastrophic earthquake or an extended drought; and the continuing cyber threat. These challenges are amplified by the increasing complexity of the energy infrastructure and systems and the interdependencies affecting other critical industries.

To further strengthen OE's ability to secure the U.S. energy infrastructure, ISER promotes the development of advanced mitigation solutions for "hardening" infrastructure against all hazards, natural and man-made. The program focuses mainly on the hazards that pose the greatest risk to the nation's energy infrastructure, including HILF events and more frequent physical threats such as devastating weather events.

Upon request, ISER also provides technical assistance to international partners, in collaboration with the U.S. Department of State, to analyze and secure energy assets.

State Energy Reliability and Assurance Grants⁶⁹

DOE proposed this grant program as a new activity for FY2016. The \$63 million proposal to establish the program was the single largest funding increase that OE requested. The program would have provided grants to states, localities, regions, and tribal entities (or groups of states and tribes). Two distinct grant programs would have been created: Grants for Electricity Transmission, Storage, and Distribution Reliability (ETSDR) and Grants for Energy Assurance. Of the \$63 million requested, \$27.5 million would have gone to the ETSDR subprogram and \$35.5 million would have gone to the Energy Assurance subprogram.

As a rationale for the program, OE's request noted that states have considerable jurisdiction over the electricity system. DOE observes that states are "excellent test beds for the evolution of the electric power system" and, with federal support, could provide innovative ways to address new trends by allowing the electric sector to provide services that meet goals for reliability,

resiliency, efficiency, environmental, and energy assurance. Such activities are in place now, but need to be adequately funded and better integrated within states and across states. DOE says that its long history of technical assistance to states has positioned it to help coordinate those planning processes within states and across state lines.

Grants for Electricity Transmission, Storage, and Distribution Reliability

DOE proposed this new program for state energy market and policy design systems to address system interdependencies and scale-up of renewable energy integration. The program was designed to support the grid modernization crosscut initiative. The requested \$27.5 million would have funded grants to states and others to develop energy system reliability plans to advance electric reliability planning and integrate the plans with environmental protection (including climate adaptation), climate resiliency, and efficiency infrastructure planning and action.⁷⁰

Energy Assurance Grants

The energy assurance planning grants would have provided formula grants to improve the short-term and long-term capacity of state, local, and tribal governments to identify the potential for energy disruptions, quantify the impacts of those disruptions, and develop responsive plans to mitigate the threat of future disruptions. The requested \$35.5 million would have been used to update energy assurance plans; require testing, training, and exercises; and ensure that plans and assessments were shared.

A key DOE rationale for the proposed program was the fact that state and local governments are ultimately responsible for responding to disasters and disruptions. This program was designed for OE to help those governments build and maintain preparedness and assurance capabilities.⁷¹ The program would have financed state, local, and tribal government efforts to enhance resiliency through energy assurance planning and the testing of, training for, and exercising of those plans.⁷² This grant program would have been undertaken in cooperation with OE's ISER program, which would have served as a convener of forums for information sharing and coordination of state energy assurance plans with other state and local disaster and emergency response plans, private sector response plans, and the plans of neighboring states.

Program Direction⁷³

This administrative activity funds the costs associated with the OE workforce, including salaries, benefits, travel, training, building occupancy, information technology services, and other related expenses. The program funding also provides for the costs associated with contractor services that support OE's mission.

End Notes

¹ The largest assets are energy production facilities, pipelines, and transmission lines.

² This mission is cited in Strategic Objective 2 of the DOE Strategic Plan.

³ DOE, FY2016 Budget in Brief, p. 32.

⁴ Prior to that time, OE programs had been managed as a minor program office under the Office of the Secretary / Office of Energy Efficiency and Renewable Energy (EERE).

⁵ DOE, QTR 2, Summary and Conclusions, p. 416, http://energy.gov/sites/prod/files/2015/09/f26/QuadrennialTechnology-Review-2015_0.pdf.

⁶ QER 2, p. 425.

⁷ DOE, Grid Modernization Multi-Year Program Plan (MYPP), November 2015 (released January 14, 2016), Executive Summary, p. xi, <http://energy.gov/sites/prod/files/2016/01/f28/Grid%20Modernization%20MultiYear%20Program%20Plan.pdf>.

⁸ DOE, Grid Modernization Multi-Year Program Plan, November 2015, p. 12.

⁹ DOE, MYPP, Executive Summary, p. xiv-xv.

¹⁰ DOE, MYPP, November 2015, Executive Summary, p. xi.

¹¹ From FY1948 through FY1977 the federal government provided an extensive amount of R&D support for fossil energy and nuclear power technologies. The energy crises of the 1970s spurred the federal government to expand its R&D programs to include renewable (wind, solar, biomass, geothermal, hydro) energy and energy efficiency technologies. In real (constant dollar) terms, funding support for all four of the main energy technologies skyrocketed during the 1970s to a combined peak in FY1979. Funding then dropped steadily, leveling off during the late 1990s. Since then, funding has increased gradually—except that the Recovery Act provided a one-year spike in FY2009. More details about DOE—and earlier (pre-1978)—spending for energy technologies are available in CRS Report RS22858, Renewable Energy R&D Funding History: A Comparison with Funding for Nuclear Energy, Fossil Energy, and Energy Efficiency R&D, by Fred Sissine.

¹² The Recovery Act funding supported smart grid activities that were authorized primarily by Title 13 of the Energy Independence and Security Act of 2007 (EISA, P.L. 110-14).

¹³ A synchrophasor is an advanced power monitoring and control device. It is also referred to as a phasor measurement unit (PMU).

¹⁴ DOE, OE, Synchrophasor Technologies and the Deployment in the Recovery Act Smart Grid Programs, August 2013, https://www.smartgrid.gov/files/Synchrophasor_Report_08_09_2013_DOE_2_version_0.pdf. For a brief discussion about synchrophasors, see the section below on Clean Energy Transmission and Reliability.

-
- ¹⁵ For an overview of the FY2016 E&W appropriations process, see CRS Report R43966, *Energy and Water Development: FY2016 Appropriations*, by Mark Holt.
- ¹⁶ Prior to 2005, DOE programs were supported partly by the E&W bill and partly by the Interior appropriations bill.
- ¹⁷ A video replay of Secretary Moniz's verbal presentation of the DOE request is available at <http://energy.gov/articles/energy-department-presents-fy16-budget-request>. The portion on energy programs, including EERE, begins at about nine minutes into the video recording. Also, the printed text of the Secretary's verbal presentation is available at <http://energy.gov/articles/secretary-monizs-remarks-presenting-department-s-fy-2016-budget-request-delivered>.
- ¹⁸ At the same time—to offset a large overall requested increase for DOE funding—the Administration sought a revenue offset derived from a proposal to repeal about \$4 billion in fossil fuel tax incentives.
- ¹⁹ See H.Rept. 114-91, *Energy and Water Development Appropriations Bill, 2016*, p. 89, April 24, 2015.
- ²⁰ H.R. 2028 as engrossed in House (passed House), p. 21.
- ²¹ S.Rept. 114-54, *Energy and Water Development Appropriations Bill, 2016*, p. 75, May 21, 2015.
- ²² The text of the enacted bill is available at <https://www.congress.gov/114/bills/hr2029/BILLS-114hr2029enr.pdf>.
- ²³ For more about smart grid and cybersecurity issues, see CRS Report R41886, *The Smart Grid and Cybersecurity—Regulatory Policy and Issues*, by Richard J. Campbell.
- ²⁴ DOE, FY2016 Budget Request (vol. 3), p. 359, http://energy.gov/sites/prod/files/2015/02/f19/FY2016BudgetVolume3_7.pdf.
- ²⁵ For more about ADMS, see the section on Smart Grid R&D, p. 14.
- ²⁶ DOE, FY2016 Budget Request (vol. 3), p. 352-353. For more about MBCS, see “Smart Grid R&D,” below.
- ²⁷ DOE, FY2016 Budget Request (vol. 3), p. 362.
- ²⁸ DOE, FY2016 Budget Request (vol. 3), p. 363-365.
- ²⁹ For FY2016, Congress approved funding to support DOE's request to establish a new program, *Transformer Resilience and Advanced Components (TRAC)*.
- ³⁰ TRAC was funded at \$5 million, which was one-half of the requested amount.
- ³¹ The CETR program is covered in DOE, FY2016 Budget Request, pp. 333-345. Note: This page reference is for DOE's PDF file available on the web—the printed version has slightly different pagination.
- ³² Improved capacity for transmission of renewable energy power generation could be important to implementing the renewable energy aspects of the Environmental Protection Agency's (EPA's) Clean Power Plan.
- ³³ These monitoring devices, also called phasor measurement units (PMUs), measure the instantaneous voltage, current, and frequency at specific locations in an electricity transmission system—usually at transmission substations. These data measurements represent the “heart-beat” and health of the power system. Voltage and current are parameters that characterize the delivery of electric power from generation plants to end-user loads, while frequency is the key indicator of the balance between electric load and generation. Thus, keeping frequency very close to 60 Hertz (cycles per second) is key to ensuring the proper operation of the power system and its reliability. For more details, see DOE, OE, *Synchrophasor Technologies and their Deployment in the Recovery Act Smart Grid Program*, 2013, p. 2, <https://www.smartgrid.gov/sites/default/files/doc/files/>

Synchrophasor%20Report%2008%2009%202013%20DOE%20%28%29%20version_0.pdf.

³⁴ See conference report, H.Rept. 111-16, p. 25.

³⁵ In this use, the term “richer” means increased frequency and amount of data made available for real-time monitoring.

³⁶ While the richer data stream improves the capability of industrial control (IC) systems, the higher speed of the automated data flow may also increase cybersecurity concerns. For more on this aspect, see CRS Report R43989, *Cybersecurity Issues for the Bulk Power System*, by Richard J. Campbell.

³⁷ NERC provides a more detailed description of “production-grade” software. See NERC, *Real-Time Application of Synchrophasors for Improving Reliability*, October 2010, p. 21, <http://www.nerc.com/docs/oc/rapirtf/RAPIR%20final%20101710.pdf>.

³⁸ The Smart Grid program is covered in DOE, FY2016 Budget Request, pp. 346-353. For more about smart grid issues, see CRS Report R41886, *The Smart Grid and Cybersecurity—Regulatory Policy and Issues*, by Richard J. Campbell.

³⁹ The smaller medium- and low-voltage lines of the electric distribution system cover more distance than high voltage transmission lines.

⁴⁰ The Smart Grid R&D Program adopts the definition of the microgrid by the Microgrid Exchange Group (MEG); namely, “A microgrid is a group of interconnected loads and distributed energy resources within clearly defined electrical boundaries that acts as a single controllable entity with respect to the grid. A microgrid can connect and disconnect from the grid to enable it to operate in both grid-connected or island-mode.” DOE, OE, Summary Report: 2012 DOE Microgrid Workshop, p. 1, <http://energy.gov/sites/prod/files/2012%20Microgrid%20Workshop%20Report%2009102012.pdf>.

⁴¹ One megawatt (MW) represents one million watts, or one thousand kilowatts.

⁴² DOE, OE, Summary Report: 2012 DOE Microgrid Workshop, p. 1. Also, see DOE, *Microgrid Activities*, <http://energy.gov/oe/services/technology-development/smart-grid/role-microgrids-helping-advance-nation-s-energysyst-0>.

⁴³ Volt/VAR optimization reduces electric line losses and increases grid efficiency. These technologies have advanced to include Volt/Volt-Ampere Reactive Optimization (VVO) sensors, equipment and software capable of reducing overall distribution line losses by 2%–5% through tight control of voltage and current fluctuations. See National Electrical Manufacturers Association (NEMA), *Volt/VAR Optimization Improves Grid Efficiency*, <https://www.nema.org/Policy/Energy/Smartgrid/Documents/VoltVAR-Optimization-Improves%20GridEfficiency.pdf>.

⁴⁴ DOE, OE, *Voices of Experience: Insights into Advanced Distribution Management Systems*, (DOE/GO-OT-6A42- 63689) February 2015, p. 3, https://www.smartgrid.gov/document/insights_advanced_distribution_management_systems.

⁴⁵ OE, *Voices of Experience*, p. 3.

⁴⁶ OE, *Voices of Experience*, p. 6.

⁴⁷ This may result in a need for regulations keyed to a more dynamic energy market.

⁴⁸ For more about transactive energy, see DOE, Gridwise Architecture Council, *Gridwise Transactive Energy Framework* (version 1.0), January 2015, http://www.gridwiseac.org/pdfs/te_framework_report_pnnl-22946.pdf.

⁴⁹ One might think of this process as a sort of “supply-response” mechanism, as a parallel concept to the growing practice of demand-response programs.

- ⁵⁰ The Cybersecurity program is covered in DOE, FY2016 Budget Request, pp. 354-360. For more about cybersecurity issues, see CRS Report R41886, *The Smart Grid and Cybersecurity—Regulatory Policy and Issues*, by Richard J. Campbell.
- ⁵¹ A probe is an action taken or an object used for the purpose of learning something about the state of the network.
- ⁵² Data exfiltration is the unauthorized transfer of sensitive information from a target's network to a location which a threat actor controls.
- ⁵³ Malware is a short-hand term for malicious software. It is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.
- ⁵⁴ The CEDS program structure also aligns with guidance provided in the 2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity, prepared by the Energy Sector Control Systems Working Group of the Critical Infrastructure Partnership Advisory Council, September 2011, http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf.
- ⁵⁵ The Energy Storage program is covered in DOE, FY2016 Budget Request, pp. 361-366.
- ⁵⁶ DOE, Grid Energy Storage, December 2013, <http://energy.gov/oe/downloads/grid-energy-storage-december-2013>.
- ⁵⁷ The Transformer Resilience and Advanced Components program is covered in DOE, FY2016 Budget Request, pp. 367-369.
- ⁵⁸ Most people have seen the round, barrel-shaped objects mounted on neighborhood electric utility poles. Those objects are transformers that reduce (step down) the current and voltage on those lines to a lower level that is appropriate for the equipment used in homes, institutions, and commercial buildings. Another familiar example of a transformer is the power adapter that often comes packaged with various consumer electronic devices such as laptop computers and computer monitors. These devices reduce, or otherwise adapt, household current and voltage to levels that won't damage sensitive electronic devices. The TRAC program focuses on much larger, grid-scale transformers.
- ⁵⁹ For more about transformer security issues, see CRS Report R43604, *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*, by Paul W. Parfomak. For more about legislation on this issue, see CRS Insight IN10425, *Electric Grid Physical Security: Recent Legislation*, by Paul W. Parfomak.
- ⁶⁰ Coronal mass ejections (CMEs) appear to pose the most serious threats to the power grid. A CME occurs when the sun ejects charged particles that interact with Earth's magnetic field, creating a "magnetic storm" that can cause long-lasting blackouts of the power grid. Scientists note that "[t]he sudden increase in power can damage sensitive electronic equipment. Power transformers can overload, causing long-lasting blackouts. Long metal structures like oil and gas pipelines can carry currents, which can enhance their corrosion over time...." See space.com, "Space Weather: Sunspots, Solar Flares and Coronal Mass Ejections," <http://www.space.com/11506-space-weather-sunspots-solarflares-coronal-mass-ejections.html>.
- ⁶¹ For instance, a single LPT that is damaged can temporarily disrupt power to 500,000 homes and, as a typically custom-designed piece of equipment weighing over 100 tons, it could take up to two years to manufacture and deliver a replacement. DOE, FY2016 Budget Request, p. 367. For more about LPTs, see DOE, *Large Power Transformers and the U.S. Electric Grid*, 2012, http://energy.gov/sites/prod/files/Large%20Power%20Transformer%20Study%20-%20June%202012_0.pdf.

- ⁶² These currents are caused by coronal mass ejections from the sun. This is a more intense experience of the same phenomenon that causes the aurora borealis, or “northern lights.”
- ⁶³ For more on this aspect, see CRS Congressional Distribution Memo, Space Weather and EMP Threats to the Electric Grid, by Richard J. Campbell.
- ⁶⁴ Harmonics are a distortion of the normal electrical current waveform, generally transmitted by nonlinear loads. Switch-mode power supplies (SMPS), variable speed motors and drives, photocopiers, personal computers, laser printers, fax machines, battery chargers and uninterruptible power supplies (UPSs) are examples of nonlinear loads.
- ⁶⁵ For more on this aspect, see CRS Report R43604, Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations, by Paul W. Parfomak.
- ⁶⁶ The National Electricity Delivery program is covered in DOE, FY2016 Budget Request, pp. 370-376.
- ⁶⁷ The most recent triennial national transmission congestion study was published in 2015. See, DOE, National Electric Transmission Congestion Study, September 2015, http://www.energy.gov/sites/prod/files/2015/09/f26/2015%20National%20Electric%20Transmission%20Congestion%20Study_0.pdf.
- ⁶⁸ The Infrastructure Security and Energy Restoration program is covered in DOE, FY2016 Budget Request, pp. 377- 386.
- ⁶⁹ The State Energy Reliability and Assurance Grants program is covered in DOE, FY2016 Budget Request, pp. 387- 391.
- ⁷⁰ More specifically, the ETSDR program would have provided planning grants to promote long-term electricity system reliability planning, including (1) integrating plans and actions for transmission, storage, and distribution (TSD) reliability, climate resiliency, and environmental compliance, (2) plans for the evolving interdependencies of electricity, natural gas and water systems; (3) regulatory reforms to enable investments in TSD that address the challenges of the evolving system, including reforms for distributed generation and energy efficiency; (4) plans for upgrades of infrastructure to make it more resilient to climate change and extreme weather; (5) design incentives and cost recovery mechanisms for reliability and climate resiliency investments; and (6) foster within-state and multi-state cooperation.
- ⁷¹ The goal of state and local energy assurance planning is to achieve a robust, secure, and reliable energy infrastructure that is also resilient—better able to withstand catastrophic events, able to restore services rapidly in the event of any disaster, and designed to diminish future vulnerabilities.
- ⁷² Such plans would have been designed to include (1) energy emergency procedures that address multiple lifeline (e.g., food, housing, and shelter) sectors, (2) integration with state energy plans, state hazard mitigation plans, and other policies, and (3) mechanisms to track the duration, response, restoration and recovery time of energy supply disruption events.
- ⁷³ The Program Direction activity is covered in DOE, FY2016 Budget Request, pp. 392-395.

Chapter 2

THE SMART GRID AND CYBERSECURITY— REGULATORY POLICY AND ISSUES•

Richard J. Campbell

SUMMARY

Electricity is vital to the commerce and daily functioning of United States. The modernization of the grid to accommodate today's uses is leading to the incorporation of information processing capabilities for power system controls and operations monitoring. The "Smart Grid" is the name given to the evolving electric power network as new information technology systems and capabilities are incorporated. While these new components may add to the ability to control power flows and enhance the efficiency of grid operations, they also potentially increase the susceptibility of the grid to cyber (i.e., computer-related) attack since they are built around microprocessor devices whose basic functions are controlled by software programming. The potential for a major disruption or widespread damage to the nation's power system from a large scale cyberattack has increased focus on the cybersecurity of the Smart Grid.

Federal efforts to enhance the cybersecurity of the electrical grid were emphasized with the recognition of cybersecurity as a critical issue for electric utilities in developing the Smart Grid. The Federal Energy Regulatory Commission (FERC) received primary responsibility for the reliability of the bulk power system from the Energy Policy Act of 2005.

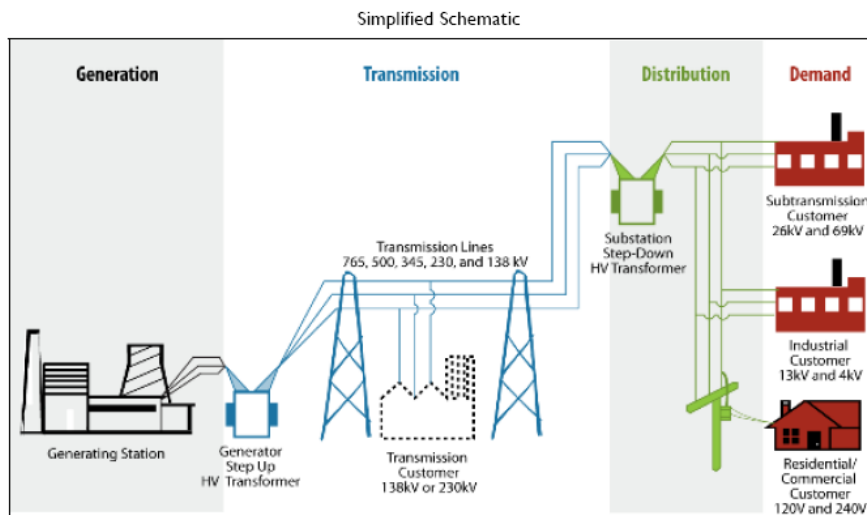
* This is an edited, reformatted and augmented version of a Congressional Research Service publication, CRS Report for Congress R41886, from www.crs.gov, dated June 15, 2011.

FERC subsequently designated the North American Electric Reliability Corporation (NERC) as the “Electric Reliability Organization” (ERO) with the responsibility of establishing and enforcing reliability standards. Compliance with reliability standards for electric utilities thus changed from a voluntary, peer-driven undertaking to a mandatory function. The Energy Independence and Security Act of 2007 (EISA) later added requirements for “a reliable and secure electricity infrastructure” with regard to Smart Grid development. NERC is also responsible for standards for critical infrastructure protection (CIP) which focus on planning and procedures for the physical security of the grid. Self-determination is a key part of the CIP reliability process. Utilities are allowed to self-identify what they see as “critical assets” under NERC regulations. Only “critical cyber assets” (i.e., as essential to the reliable operation of critical assets) are subject to CIP standards. FERC has directed NERC to revise the standards so that some oversight of the identification process for critical cyber assets was provided, but any revision is again subject to stakeholder approval. While reliability standards are mandatory, the ERO process for developing regulations is somewhat unusual in that the regulations are essentially being established by the entities who are being regulated. This may potentially be a conflict of interest, especially when cost of compliance is a concern, and acceptable standards may conceivably result from the option with the lowest costs. Since utility systems are interconnected in many ways, the system with the least protected network potentially provides the weakest point of access.

Cybersecurity threats represent a constantly moving and increasing target for mitigation activities and mitigation efforts could likewise spiral upward in costs. Recovery of costs may present a major challenge especially to distribution utilities and state commissions charged with overseeing utility costs. EISA only requires states to consider recovery of costs related to Smart Grid systems. FERC has jurisdiction over the bulk power grid, and cannot compel entities involved in distribution to comply with its regulations. Recoverability from a cyber attack on the scale of something which could take down a significant portion of the grid will likely be very difficult, but maintaining a ready inventory of critical spare parts in close proximity to key installations could quicken recovery efforts from some types of attack. The electricity grid is connected to (and largely dependent on) the natural gas pipeline, water supply, and telecommunications systems. Technologies being developed for use by the Smart Grid could also be used by these industries. Consideration could be given to applying similar control system device and system safeguards to these other critical utility systems.

INTRODUCTION

Electricity is vital to the commerce and daily functioning of United States. The electrical grid of the United States consists of all the power plants generating electricity, together with the transmission and distribution lines and their associated transformers and substations which bring power to end-use customers. Electric power generation in the United States is currently dominated by the use of combustible fuels, such as coal and natural gas, or from biomass. These fuels are burned to produce steam in boilers which is used to turn turbine-generators which produce electricity. Nuclear power uses heat from the decay of radioactive elements to produce steam. However, electricity can also be generated directly by wind turbines, solar power, geothermal energy, and hydropower. Figure 1 illustrates the phases of the electric power production process. Electricity from large central station power plants is routed to a step-up transformer which raises the voltage so the power can be sent over high-voltage transmission lines to step-down transformers in substations which then transfer this energy at lower voltages via distribution lines to industrial, commercial, and residential users.



Source: CRS, based on graphic found at <https://reports.energy.gov/BlackoutFinal-Web.pdf> (p. 5).

Figure 1. Elements of the Electric Power System.

Generally, electricity must be used as soon as it is produced because large amounts of electricity cannot be easily stored.

Originally, the individual company systems were not linked, but with greater electricity demand came the necessity of sharing generation resources. This sharing of generation resources required an interconnection of separate company systems to enable power sales and transfers. These aggregated power systems form three major “interconnections”—the Eastern and Western interconnections, and the Electric Reliability Council of Texas which includes most of the state of Texas. Within these interconnections are reliability regions, and a number of balancing authorities¹ which “integrate resource plans ahead of time, maintain load-interchange generation balance” within a balancing authority area, and “support interconnection frequency in real-time.”² The grid also connects the many publicly and privately owned electric utility and power companies in different states and regions of the United States³ (and in Canada and Mexico).

Congress passed the Public Utility Regulatory Policies Act of 1978 (P.L. 95-617) which allowed non-utility power producers into wholesale power markets (e.g., for the sale of electricity to entities other than the end-user of power). The passage of the Energy Policy Act of 1992 (P.L. 102-486) served to further promote greater competition in the bulk power markets.⁴ As a result, in many parts of the United States, the electric power industry began to transition from highly regulated, local monopoly companies which generated, transmitted, and distributed electricity to end-use customers, to a business in which power generation is competitive while the industry’s transmission and distribution functions are still highly regulated. While the federal government regulates the electric power transmission function and wholesale power markets, regulation of the distribution function of the electric power business is still largely carried out by state government agencies.

Much of the infrastructure which serves the U.S. power grid is aging. The average age of power plants is now over 30 years; most of these facilities were originally designed to last 40 years.⁵ Electric transmission and distribution system components are similarly aging, with power transformers averaging over 40 years of age,⁶ and 70% of transmission lines being 25 years or older.⁷ As components of the system are retired, they are replaced with newer components often linked to communications or automated systems.

With changes in federal law,⁸ regulatory changes, and the aging of the electric power infrastructure as drivers, the grid is changing from a largely patchwork system built to serve the needs of individual electric utility companies to essentially a national interconnected system capable of

accommodating massive transfers of electrical energy between regions of the United States. The modernization of the grid to accommodate today's power flows, serve reliability needs, and meet future projected uses is leading to the incorporation of information processing capabilities for power system controls and operations monitoring. The "Smart Grid" is the name given to the evolving electric power network as new information technology systems and capabilities are incorporated. While these new components may add to the ability to control power flows and enhance the efficiency of grid operations, they also potentially increase the susceptibility of the grid to cyber (i.e., computer-related) attack since they are built around microprocessor devices whose basic functions are controlled by software programming and subject to manipulation over a network.

The information processing attributes which make the smarter grid attractive are the very same attributes which can increase the vulnerability of the electric power system and its critical infrastructure to a potentially devastating cyber attack. The potential of the Smart Grid to revolutionize the ways power is generated and used is great, but so too are the potential risks if not sufficiently addressed.

The Energy Independence and Security Act of 2007⁹ (EISA) (P.L. 110-140) defined the attributes of a Smart Grid and plans for its development. The potential for a major disruption or widespread damage to the nation's power system from a large scale cyberattack has increased focus on the cybersecurity of the Smart Grid. While a nation-state might have the resources and capability to create widescale disruption of the U.S. grid (to create economic disorder or as part of a physical attack), terrorists or hackers are less likely to have the sophistication or resources necessary to inflict damage on a national scale. But the possibility of collaboration between terrorists and hackers could increase the capability of these groups to launch network-based cyberattacks against critical U.S. infrastructure.¹⁰

Among the issues for Congress is whether the existing requirements of current law adequately assure the cybersecurity and reliable operation of the U.S. electricity grid today (and the Smart Grid of tomorrow). This report will look at issues key to these determinations, discussing the scope and point of application of regulations, and where the overall responsibility rests for the cybersecurity of the grid.

ATTRIBUTES OF A SMART GRID

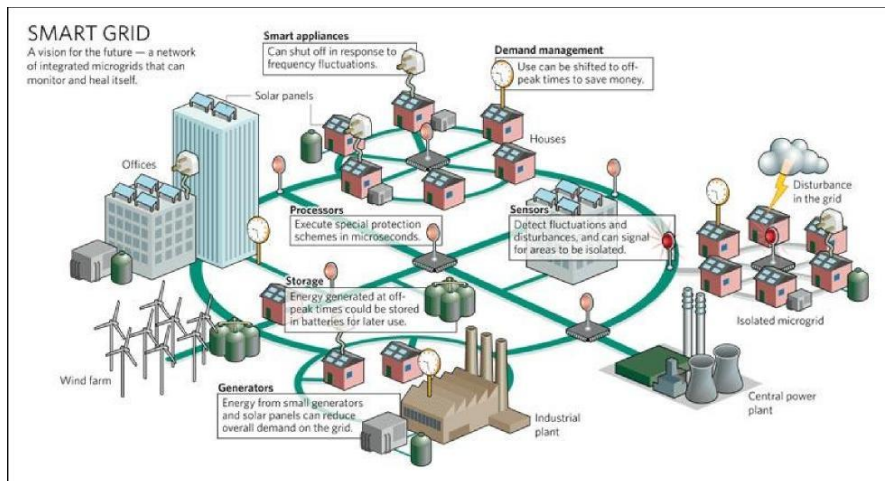
The U.S. Department of Energy (DOE) summarized its view of the potential of the Smart Grid by the year 2030 as:

... a fully automated power delivery network that monitors and controls every customer and node, ensuring a two-way flow of electricity and information between the power plant and the appliance, and all points in between. Its distributed intelligence, coupled with broadband communications and automated control systems, enables real-time market transactions and seamless interfaces among people, buildings, industrial plants, generation facilities, and the electric network.¹¹

A “smarter” grid is gradually being introduced as upgrades to the systems and components of the power generation, transmission, and distribution infrastructure. Substation and distribution substations are being automated with superior switching capabilities to enhance current flows and control of the grid. Devices called “phasor measurement units” are also being added to substations to make time and location-specific measurements of transmission line voltage, current, and frequency (i.e., synchrophasor measurements made 30 times per second instead of data measured once every two to four seconds by current industrial control systems) providing better tools to improve power system reliability.¹² DOE’s strategic plan targets the deployment of 1,000 phasor measurement units by 2013.¹³

Advanced meters are being introduced in some utility markets which can offer customers the ability to leverage demand response¹⁴ regimes and technologies, and potentially benefit from the interactive features of the Smart Grid by shifting their energy use to off-peak hours. Expectations vary of what a Smart Grid could accomplish, and the estimated costs of a system rise with the increased scope and attributes of a system. Some see the Smart Grid as only an enhancement of today’s existing transmission and distribution systems focused on improving the reliability and efficiency of the grid. Others see the Smart Grid of the future as an integrated system spanning the nation from coast to coast, able to seamlessly combine distributed resources and central power stations across the three major interconnections¹⁵ of the U.S. grid. Under such a vision, distributed and renewable energy resources could be efficiently integrated into the grid, with power from (for example) intermittent wind generation channeled by sensors and intelligent electronics from multiple widely dispersed sites to where power is needed anywhere on the grid. *Figure*

2 shows a possible configuration of a Smart Grid system illustrating components of an interconnected, two-way intelligent network, and distributed and central station sources of power. The efficiency and economy of all grid operations could conceivably be optimized by similarly harnessing all power generation to take advantage of a wide range of generation and storage resources across the United States.



Source: Consumer Energy Report. See <http://www.consumerenergyreport.com/wp-content/uploads/2010/04/smartgrid.jpg>.

Figure 2. One Conceptualization of the Smart Grid.

DEFINING CYBERSECURITY FOR THE SMART GRID

A prolonged disruption of energy from the grid was described in a report for the Presidential Commission on Critical Infrastructure¹⁶ as an event which would seriously affect every infrastructure, with the possibility of a cyberattack causing such damage considered as a possibility.

The widespread and increasing use of Supervisory Control and Data Acquisition¹⁷ (SCADA) systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means. The exponential growth of information system networks that interconnect the business, administrative, and operational systems contributes to system vulnerability.¹⁸

EISA gave the National Institute of Standards and Technology (NIST) the role of coordinating the development of a framework to enable the development of the Smart Grid in a safe and secure manner, and NIST issued its first guidelines for cybersecurity of the Smart Grid in 2010. Because cybersecurity threats were perceived as “diverse and evolving,” NIST advocated a defense-in-depth strategy with multiple levels of security because no single security measure could counter all types of threats.¹⁹ The key to NIST’s suggested approach is the determination of risk (i.e., the potential for an unwanted outcome resulting from internal or external factors, as determined from the likelihood of occurrence and the associated consequences) as quantified by the threat (e.g., event, actor or action with potential to do harm), the vulnerability (e.g., weakness in the system), and the consequences (e.g., physical impacts) to the system.²⁰

CYBERSECURITY VULNERABILITIES OF THE SMART GRID

A smarter grid is largely the result of the modernization of the grid. Most sectors of business and industry have gone from the analog age of knobs and dials to the digital age of sensors and electronic displays in the recent past, and that process is now reaching into the nation’s electric power infrastructure. Part of the delay has been due to the long-lived nature of the capital assets which make up the industry. The power plants and other expensive components of the grid can function for many productive years if maintenance of the systems is kept up. However, much of the delay in modernization has been due to cost concerns, as many electric utilities seek to manage expenses by delaying replacement of aging systems as long as possible. Several of the better-known vulnerabilities of a smarter grid are discussed in the following paragraphs.

Control Systems

Industrial control (IC) systems are particularly vulnerable to cyberattack because of their intelligence and communications capabilities. IC systems perform a number of functions in the electrical grid, ranging from microprocessor-based control systems which control the actuation and operation of one or more devices, to more sophisticated industrial IC systems which can manage entire industrial processes or automated systems. SCADA

systems are a well-known application of remote IC used to monitor and control electric transmission system components.

While cyber-intrusions into the U.S. grid have been reported in recent years,²¹ no impairment or other damage has been publicly reported as a result of the attacks. By exploiting loopholes in cybersecurity, cyberattackers could breach the privacy of customers power usage data and access large numbers of meters, perhaps sending deliberately misleading information to the grid. This could potentially overload systems or cause grid operators to respond to false readings. However, concerns exist as to the potential damage that could result in the future from malware left behind by such intrusions or doorways created in systems which could be exploited.²² The revelation of the complexities of the Stuxnet worm²³ and the alleged targeting of the control systems of a nuclear power plant in Iran²⁴ have raised additional concerns about the vulnerability of electric power systems worldwide.

The Stuxnet worm reportedly affected the logical decision making functions of the control systems of one particular type of manufacturing facility. Theoretically, Stuxnet-like malware could be adapted to impair other types of process or control systems in malicious or unpredictable ways. Malware modified in such ways could overload and damage targeted equipment and systems in critical infrastructure.²⁵ The Department of Homeland Security (DHS) conducted a simulated cyberattack on an electric generator control room and partially destroyed a large diesel-electric generator secured for the test as a demonstration of existing power system vulnerabilities.²⁶

Connections through Other Systems

Utilities have routinely accessed control systems either wirelessly or by telephone lines for many years. In fact, telephone lines often used to access corporate systems may even provide access to utility control systems. A recent GAO report highlighted vulnerabilities at the Tennessee Valley Authority, a large federal utility in the United States.

... the interconnections between TVA's control system networks and its corporate network increased the risk that security weaknesses, on the corporate network could affect control systems networks and we determined that the control systems were at increased risk of

unauthorized modification or disruption by both internal and external threats.²⁷

Communications and Internet Access

Grid devices capable of two-way communications are considered to be potential points of unauthorized system access, and can represent a potential cybersecurity vulnerability. While security protocols may exist to prevent unauthorized entry, wireless networks can be monitored and potentially hacked by cybercriminals. Smart meters are another example of new applications in which the security of data has been mentioned as a concern. At the heart of smart meters are semiconductor chips which allow data about energy use to be sent wirelessly to the electric distribution company, and which potentially allows the meter to control the flow of power to customers. The security of the encrypted information in the communications protocol used by many of these devices has been questioned in the past, and questions have been raised about the effectiveness of efforts to patch identified flaws. The primary consideration in the choice of wireless protocol by semiconductor providers seems to be cost of the system, a criteria which is not always compatible with cybersecurity goals for secure communications.²⁸ While the developing Smart Grid is likely to use today's internet and wireless communications systems for many years to come, security concerns and data usage requirements may move the system to dedicated communications and information channels serving uniquely Smart Grid uses.

Potential access to SCADA systems via the Internet has often been cited as a key vulnerability for electric power systems. Hackers have used the Internet to launch denial of service,²⁹ phishing,³⁰ and various other forms of cyberattack. The effective recording, processing, and exchanging of data is becoming increasingly critical to the reliability of the power system,³¹ and deliberately introduced misinformation can be damaging. Internet-linked communications systems may be important to today's interconnected grid, but the Internet also provides a ready path to cyberattack from any corner of the world wide web.

Combined Cyber- and Physical Attacks

The vulnerability of key components of the grid to a physical attack has been long known, but a coordinated and sustained physical and/or

cyberattack³² could be problematic. After a cyberattack, restored systems may be repaired and protected against known vulnerabilities, but a coordinated cyberattack over a short time period targeting different Smart Grid systems could slow recovery. The same would hold true for repeated physical attacks, or combined cyber- and physical attacks on key grid components. Under such circumstances, the resources of emergency programs in place to replace important grid systems and components (such as the Edison Electric Institute's "Spare Transformer Equipment Program"³³) may not be adequate to provide enough replacement parts to fully restore reliable grid operations in a timely manner.

Supply Chain

The components of smarter grid devices present another potential vulnerability concern. Most of the smart meter, sensor, and other equipment makers are international companies who obtain their components from international sources. Taiwan, Singapore, China, and South Korea are among the largest overseas manufacturers of semiconductors and microprocessors for smart devices. The reliable operation of semiconductor and microprocessor-based devices is based on the low-level firmware³⁴ controlling the device's basic functions. Firmware in the form of fixed machine-language binary code is found in almost all the electronic devices making up smarter grid products such as programmable controllers and programmable logic arrays. If a hacker or cybercriminal gained access to such devices (especially during the manufacturing process), a section of code could be covertly inserted in the device and activated in such a way as to impair its functioning in a reliable manner. Some might suggest random or statistically based testing of the firmware in smarter grid devices. But the impairment would not need to be placed in all such devices coming off an assembly line. If a large enough sample was impaired, the effect might be enough to cast doubt on the reliability of a whole class of such devices.

Geomagnetic Impairment

An electromagnetic pulse (EMP) is a large burst of electromagnetic radiation resulting from the detonation of a nuclear weapon or from other means. EMPs can cause voltage and current surges which can severely damage

electrical equipment and systems. A high-altitude nuclear explosion could cause an EMP which could severely impair an electric power system not shielded from the effects of an EMP.

However, deliberate, large-scale, man-made attacks are not the only potential threat which could take down a substantial portion of the electric grid. Radiation or charged particles ejected into space weather from solar flare eruptions could cause geomagnetic storms which could interfere with telecommunications networks or damage orbiting satellites. Periodically, these eruptions from the sun are powerful enough to disrupt the operations of electric power systems. Solar flares occur in cycles of almost 11 years.³⁵ Occasionally, severe space weather results in a huge eruption of particles which can be particularly disruptive to electric power systems, and induce ground currents powerful enough to actually melt the copper windings of electric power transformers. The last major solar flare eruption in 1989 caused blackouts across the Canadian province of Quebec for nine hours. But even greater storms can occur perhaps every 100 or more years. The first major eruption of this size was observed in 1859. It destroyed much of the world's telegraph infrastructure of the time. Another event observed in 1921 demonstrates that although these events are rare, they are likely to occur again and could have tremendous societal and economic impacts for the United States:

... the occurrence today of an event like the 1921 storm would result in large-scale blackouts affecting more than 130 million people and would expose more than 350 transformers to the risk of permanent damage.³⁶

It could take weeks or months to replace most of the damaged transformers. Some of the larger units could take years to replace due to the fact there are no U.S. power transformer manufacturers,³⁷ and a multi-year backlog exists for the larger units.

CURRENT CYBERSECURITY POLICY FOR THE SMART GRID

A smarter grid is increasing reliance on automated systems to manage energy sources, power control devices, system information, and power flows. Automation will allow information from smarter processors and sensors to be

processed at much faster rates, giving power system operators more accurate and timely information, and giving customers greater input into their own power use. But, the possibility that such systems could be hijacked in such a way as to bring down the grid regionally or even nationally, and cause long-term damage to critical systems and components, is giving Congress reason to consider the cybersecurity of the electric power infrastructure.

The passage of the Homeland Security Act of 2002 (P.L. 107-296) (HSA) established the Department of Homeland Security. HSA increased penalties for certain computer-based crimes, and in addition to improving on the earlier Computer Fraud and Abuse Act of 1986,³⁸ made critical infrastructure protection a key mission of DHS.

Federal efforts to enhance the cybersecurity of the electrical grid were reemphasized with the recognition of cybersecurity as a critical issue for electric utilities in developing the Smart Grid. The Energy Independence and Security Act (EISA) of 2007 (P.L. 110-140) thus added requirements for “a reliable and secure electricity infrastructure” with regard to Smart Grid development. EISA directed NIST to develop a framework for protocols and standards for the Smart Grid to achieve “interoperability”³⁹ of devices and systems. The American Recovery and Reinvestment Act of 2009 (P.L. 111-5) provided NIST with funds to proceed with this mandate.

Status of Regulatory Implementation

NIST issued a report, “NIST Framework and Roadmap for Smart Grid Interoperability Standards” (NIST SP 1108, January 2010), listing 75 existing standards which are likely to be applicable for an interoperable Smart Grid, and identified 15 high-priority gaps and harmonization issues. NIST also issued a “Smart Grid Cybersecurity Strategy and Requirements” report (NISTIR 7628, September 2010) assessing requirements to ensure the security and reliability of a modernized grid. This report also classified Smart Grid interfaces according to potential impacts that could result from compromise of these systems.

The Federal Energy Regulatory Commission (FERC or the Commission) received primary responsibility for the reliability of the bulk power⁴⁰ system from the Energy Policy Act of 2005 (EPACT05) (P.L. 109-58). EPACT05 also gave FERC the authority to commission an “Electric Reliability Organization” (ERO) to establish and enforce reliability standards. FERC subsequently designated the North American Electric Reliability Corporation (NERC) as the

ERO. Compliance with reliability standards for electric utilities thus changed from a voluntary, peer-driven undertaking to a mandatory function. While NERC is responsible for standards for the bulk power system in the United States, it is also seeking recognition by applicable governmental authorities in Canada and Mexico to establish and coordinate reliability standards for the bulk power systems of these respective countries.⁴¹ NERC is also responsible for standards for critical infrastructure protection (CIP) which focus on planning and procedures for the physical security of the grid. NERC has delegated much of the daily process of maintaining reliability of the grid to regional entities via delegation agreements which are subject to FERC approval. Compliance and enforcement with NERC standards is therefore largely a responsibility of these regional entities, which are mostly responsible for imposing penalties for violation of reliability standards.⁴² NERC's CIP standards essentially approach cybersecurity as an extension of reliability, and address nine areas including *Sabotage Reporting*, *Critical Cyber Asset Identification*, and *Electronic Security Perimeters*, and *Recovery Plans for Critical Cyber Assets*.⁴³ These standards identify what utilities must do to protect "cyber assets"⁴⁴ seen as critical to the reliability of the bulk power⁴⁵ system.

EISA directed FERC to work with NIST in developing Smart Grid interoperability standards, and required FERC to institute a formal rulemaking process to adopt interoperability (including cybersecurity) standards when FERC was satisfied that a consensus on defining the standards had been reached. NIST advised FERC in October 2010 that it had identified five "foundational" sets of standards⁴⁶ which may allow FERC to go forward with instituting rulemaking proceedings to adopt standards to ensure Smart Grid functionality, interoperability, and cybersecurity. The standards would be updated as Smart Grid requirements and technologies evolve.

FERC held a technical conference in January 2011 to determine if there was "sufficient consensus" that the five sets of standards proposed by NIST were adequate for standards and protocols to be adopted. The comments of conference participants showed that a consensus on the standards had not in fact been reached with several participants stating that they were unsure of what would constitute a consensus, and questioning whether such standards would then automatically become "mandatory and enforceable." FERC issued a supplemental notice in February 2011 (requesting all comments by April 2011) to aid the Commission's determination as to whether a consensus exists on the proposed NIST interoperability standards. Additional questions were asked in the notice to solicit opinions on related topics including the NIST

process for determining the readiness of a standard with regards to interoperability and cybersecurity, whether making standards enforceable would achieve interoperability goals, how testing and certification of cybersecurity requirements could be incorporated into the standards process, and whether the Commission should consider different criteria for evaluating interoperability and functionality (and the extent to which cybersecurity is an element of each).⁴⁷

Assessment of Cybersecurity Progress by Government Accountability Office

Congress asked the U.S. Government Accountability Office (GAO) to assess progress by NIST and FERC on Smart Grid cybersecurity guidelines and standards. GAO issued a report with its findings in January 2011.⁴⁸ GAO found that NIST has largely addressed “key cybersecurity elements” such as the cybersecurity risks of Smart Grid systems and had identified security controls essential to such systems. GAO also found that NIST had not addressed the risks of attacks on Smart Grid systems using both cyber- and physical means. GAO recommended that NIST finalize its plan and schedule for updating its cybersecurity guidelines to include these elements.

GAO also pointed out that while EISA had given FERC authority to adopt Smart Grid standards, it did not give FERC specific enforcement authority over implementation of standards. GAO recognized that a regulatory divide exists between federal, state, and local entities on various aspects of Smart Grid interoperability and cybersecurity. As such, GAO states that such standards will remain voluntary unless regulators use other authorities to enforce standards compliance. GAO recommended that FERC develop a coordinated approach (with other regulatory jurisdictions) to monitor voluntary standards and address any gaps in compliance.

FERC and NIST agreed with GAO’s recommendations.⁴⁹ However, FERC Chairman Wellinghoff stated that while a coordinated approach would be pursued, FERC may lack the authority to address any gaps in compliance, and that this being the case, Congress may want to consider the matter further. Furthermore, in addressing GAO’s comments, the Chairman broached the question of whether other-than-voluntary compliance with Smart Grid standards by “relevant manufacturers and utilities” is what Congress intended in EISA.⁵⁰

Meanwhile, NIST has communicated to FERC its own concerns that under the existing process, it could take years for the Commission to adopt rules on the many individual standards needed to achieve interoperability of

the Smart Grid while recognizing that many “customized” upgrades to the grid continue to be installed. NIST suggested that in the absence of formal standards, FERC could request “interoperability roadmaps” from utilities to determine if they addressed interoperability based on the NIST framework in the utilities’ grid modernization efforts.⁵¹

Assessment by DOE’s Inspector General of FERC’s Monitoring of Grid Cybersecurity

The DOE Inspector General released an audit report⁵² in January 2011 of FERC’s monitoring of grid cybersecurity, with regard to the Commission’s responsibilities under EPACT05. The report found that CIP cybersecurity standards developed “did not include a number of security controls commonly recommended for government and industry systems,” and criticized FERC’s oversight of the process for developing these standards, citing a need for FERC to use its existing authority to ensure timely standards development to address emerging security threats. The report also said that FERC’s implementation approach and schedule for CIP standards did not adequately consider risks to information systems, since FERC was focusing on documentation of controls rather than implementation of controls. FERC was advised to revise its focus to ensure that controls to address higher threat risks are given priority. The report noted that these problems existed, in part, because the Commission had “only limited authority” to ensure cybersecurity over the bulk electric system, and could not implement its own reliability standards or issue alerts. However, the report went on to conclude that even “when such authority did exist,” FERC did not always act “to ensure that cybersecurity standards were adequate.”

FERC Chairman Wellinghoff mostly concurred with the report’s recommendations⁵³ while noting that “the current statutory framework is adequate for addressing emerging cybersecurity threats through mandatory standards.” The Chairman stated that FERC will make every effort “to approve CIP standards as soon as possible after they are developed by NERC.”⁵⁴

Policy Concerns

Self-determination is a key part of the CIP reliability process. Utilities are allowed to self-identify what they see as “critical assets”⁵⁵ under NERC regulations. While compliance with CIP standards became mandatory in 2010, FERC mandated modifications to the criteria defining critical assets for

reliability purposes. Only “critical cyber-assets” (i.e., as essential to the reliable operation of critical assets) are subject to CIP standards. FERC directed NERC to revise the standards so that some oversight of the identification process for critical cyber-assets was provided, but any revision is again subject to stakeholder approval. Under current law, FERC cannot issue its own reliability standards.

While reliability standards are mandatory, the ERO process for developing regulations is somewhat unusual in that the regulations are essentially being established by the entities who are being regulated.⁵⁶ This can potentially be an issue when cost of compliance is a concern, and acceptable standards may conceivably result from the option with the lowest costs. While FERC ultimately has approval authority over the regulations NERC submits and can remand such regulations it judges as not satisfying requirements, any such revisions are ultimately subject to NERC stakeholder approval. NERC standards could therefore be seen as a minimum threshold for compliance, as some utilities may choose to go beyond what is minimally required. But since utility systems are interconnected in many ways, the system with the least protected network potentially provides the weakest point of access.

OTHER ISSUES IN FEDERAL SMART GRID CYBERSECURITY POLICY

Legacy Systems

Legacy devices and systems (such as many SCADA and substation automation systems) may represent as much of a vulnerability to cybersecurity as new Smart Grid components. They were not designed with cybersecurity in mind, and are often interconnected either via the Internet or by other, sometimes “unsecured” avenues. DOE describes the legacy system communications issue as follows:

The legacy communication methods that now support grid operations also provide potential cyber attack paths. Many cyber vulnerabilities have been identified by cyber security assessments of SCADA systems. Power grid substation automation and security have also recently been evaluated. The level of automation in substations is increasing, which can lead to more cyber security issues. The cyber security issues identified during the assessments and evaluations need to be resolved, but the

known issues should not be construed as a complete assessment of the current power grid security posture.⁵⁷

Some legacy grid devices are being retrofitted with communications capabilities to allow them functionality in the smarter grid, or permit easier maintenance, potentially introducing grid vulnerabilities which may not have existed before. NIST has suggested the establishment of “Priority Actions Plans” to resolve interoperability issues between legacy equipment and Smart Grid systems as these are installed.⁵⁸

FERC specifically rejected proposals by commenters for additional interoperability standards (at this time) addressing existing resources or equipment and cost-effective integration of legacy equipment, and interfaces between utilities.⁵⁹ Replacement of these systems is recognized by FERC as a possible option for utilities to apply for recovery of the “stranded costs” of legacy systems replaced by Smart Grid investments.⁶⁰

Leadership of Federal Authority for Smart Grid Cybersecurity

The issue of which, or whether, a single federal agency should have ultimate authority over Smart Grid cybersecurity remains largely unresolved. DHS, DOE, and FERC have all either stated claims or been mentioned as candidates for overall leadership of the issue based upon implications to national security, energy policy and technology leadership, or industry understanding and organizational mission, but the current missions of these agencies is only the starting point for a discussion. Since Smart Grid devices are being installed beyond the federally regulated power grid, the system could potentially face intrusions from cyberattacks initiated on less-protected distribution systems. Leadership of Smart Grid and cybersecurity issues may require the ability to communicate issues and push solutions in forums beyond federal jurisdictions if the goal is to protect against cyber-threats to the grid for the entire United States.

DHS’s mission to protect national security against cyber-threats currently centers on “civilian government systems” and DHS works with industry to “secure critical infrastructure and information systems.” DHS is focused on analyzing cyber-threats and reducing vulnerabilities, and distributing information on potential cyberattacks to ensure the safety of cybersystems.⁶¹ DHS will distribute warnings of cyber-threats to other federal agencies, state and local governments and to industry.

DOE has the technical and research capabilities of the national laboratories to draw upon with regard to cybersecurity and the Smart Grid, as well as its own internal policy offices which deal with an array of electricity system issues. DOE has worked with electric utilities to understand the cyber-vulnerabilities of the grid, and has tasked the national laboratories with helping to develop technologies and software patches to identify problems and harden legacy control systems against potential cyber-intrusions.

FERC is an independent, self-funded regulatory agency within DOE, with statutory authority over major aspects of the wholesale electric, natural gas, hydroelectric, and oil pipeline industries.⁶² As such, FERC's responsibility for the reliability of the grid and related ratemaking authority allow the Commission to discover issues and authorize utilities to recover the jurisdictional portion of costs related to grid critical infrastructure protection upgrades. FERC recognizes that EISA does not make Smart Grid standards mandatory, nor does EISA give it authority to make or enforce such standards.⁶³ FERC has jurisdiction over the bulk power system, but this currently excludes authority over the nation's electric distribution systems where much of the smarter grid will be deployed. The Commission appears to view its reliability mandate under EISA as giving it the authority to adopt Smart Grid standards which will be applicable to all electric power facilities and devices with Smart Grid features, including those at the distribution level. FERC further ties cybersecurity to reliability by proposing a "harmonization" of each Smart Grid protocol and reliability standard developed.⁶⁴

Cost Challenges of Maintaining a Cyber-Secure Smart Grid

Cybersecurity threats present a constantly moving and growing need for mitigation activities. As new devices and systems are being developed for the Smart Grid, so too is the array of infrastructure elements which must potentially be protected. This is a key concern for utilities, as the resources which may have to be applied to cybersecurity concerns could likewise spiral upward in growth and costs. Utilities may understand how a smarter grid can enhance their efficiency and reliability, and the need for cybersecurity safeguards. Commercial and industrial customers may also see potential benefits in Smart Grid-enabled programs (such as demand response), and it is likely they will fund a significant portion of smarter grid improvements through rates. But at present very few consumers at the residential level seem to understand the potential of the Smart Grid, or have reason to believe it can

do anything for them except increase rates.⁶⁵ One recent study expects cybersecurity spending to represent approximately 15% of total Smart Grid capital investment between 2010 and 2015 (with total investment estimated to be \$1.5 billion in North America).⁶⁶

Smart Grid enhancements across the United States may vary by utility, state, region, and regulatory jurisdiction. Recovery of costs may present a major challenge especially to distribution utilities and state commissions charged with overseeing utility costs. When faced with such decisions, the perception of the potential risks to the utility's local system will likely bear on what costs the utility's ratepayers should pay. EISA requires states only to consider recovery of costs related to Smart Grid systems. FERC has jurisdiction over the bulk power grid, i.e., transmission and wholesale rates in interstate commerce. FERC cannot compel entities involved in distribution to comply with its regulations. Since distribution utilities are regulated by state or local public utility commissions, Smart Grid investments will likely require approval by these jurisdictions. The issue of whether Smart Grid standards for interoperability should be voluntary or mandatory for these jurisdictions remains unresolved.

Privacy and Data Security

The sharing of information in applications used by the smarter grid has raised questions on the safety of that information. Security of customer information in wireless applications, and how personal data characteristics (such as customer usage information) can be protected are issues often mentioned in discussions of the Smart Grid and cybersecurity. Encryption of data (with limited decryption for data checking), and aggregation of data at high levels to mask individual usership have been mentioned as ways to protect the identity of individual customers. Limiting the amount of data to just information needed for billing purposes has been suggested as a remedy to the potential for misuse of data.⁶⁷ Real-time monitoring of these networks may alert system operators to suspicious activities. But even these methods might not be enough to guard against a sophisticated intruder if data security is taken for granted. The development of Smart Grid standards for electric utilities and their partners governing the collection and use of customer data may be a possible next step.

If customers participate in demand-side management programs, then customer usage data can provide a wealth of information for a variety of

programs for interruptible loads or time-of-use rates. But customer-specific data stored in home area networks (HANs), or customer-specific data communicated between the HAN and distribution utility (or load aggregator) must be secure to protect the privacy of information. The advent of electric vehicles may offer another potential payload of data on customer movement and habits, if data collected or stored is not restricted to electricity consumption for billing purposes.

The National Regulatory Research Institute recommended in a recent report⁶⁸ that public utility commissions should define the information which utilities will collect, determining with whom and for what purpose it should be shared, and assess the need for protecting the data. While allowing states to develop their own policies may be accomplished more quickly, the report also advocates for a national approach to Smart Grid privacy issues.

DOE has worked with electric utilities and the Electric Power Research Institute (EPRI) to develop profiles for Smart Grid products to address concerns about data privacy. These profiles are meant to provide guidance on how to build cybersecurity into Smart Grid applications under development, so that they can be more securely integrated into the Smart Grid.⁶⁹

Government-Industry Coordination on Threats

In 2010, the Edison Electric Institute (EEI) issued its own “Principles for Cyber Security and Critical Infrastructure Protection”⁷⁰ to discuss development of a framework for addressing cybersecurity threats. EEI, the trade association of U.S. shareholder-owned electric utilities, suggested a coordinated effort of government, industry, and suppliers of critical grid systems and components was necessary to protect the grid from cyberattacks as a “shared responsibility.” EEI believes that the sharing of intelligence on evolving threats and a clear plan of action on imminent threats is key to this arrangement. EEI also expects that such a policy would help protect national security and the public welfare, and aid in the prioritization of assets which need enhanced security. EEI expects that such a partnership could “utilize all stakeholder’s expertise,” allowing owners and operators of critical infrastructure to propose mitigation strategies that will avoid significant adverse consequences to utility operation or assets.

OTHER COLLABORATIVE CYBERSECURITY INITIATIVES

There are a number of collaborative efforts involving private sector, academia, national laboratories, consumer groups, and others looking at cybersecurity and Smart Grid issues. Federal agencies are also working together to ensure communication and share resources on these issues, and helping to fund industry cybersecurity initiatives.⁷¹ Two of the major DOE-led initiatives are discussed below.

DOE is home to the Federal Smart Grid Task Force (FSGTF) established under EISA to “ensure awareness, coordination, and integration of the diverse activities of DOE’s Office of Electricity Delivery and Energy Reliability (OE) and elsewhere in the federal government related to Smart Grid technologies, practices, and services.”⁷² FERC, the Department of Commerce, the Environmental Protection Agency, the Department of Agriculture, and the Department of Defense are also members of the FSGTF.

DOE also funds (with OE leading DOE’s participation) the “Trustworthy Cyber Infrastructure for the Power Grid” (TCIPG) initiative, working with DHS and industry.⁷³ TCIPG is led by the academic sector as a public-private research partnership, supporting the development of resilient and secure Smart Grid systems, leveraging research previously funded by the National Science Foundation:

TCIPG’s research plan is focused on securing the low-level devices, communications, and data systems that make up the power grid, to ensure trustworthy operation during normal conditions, cyber-attacks, and/or power emergencies. At the device level, new key functionality is being designed in hardware in order to detect attacks and failures and to restore proper system operation. Likewise, virtual machine technology is being developed and adapted for advanced power meters in order to permit new power use scenarios while preserving privacy. At the protocol level, new techniques are being developed to detect, react to, and recover from cyber attacks that occur while preserving integrity, availability, and real-time requirements.

Participating in TCIPG are the University of Illinois at Urbana-Champaign, Dartmouth College, Cornell University, the University of California at Davis, and Washington State University. Current TCIPG projects are focused on developing “trustworthy cyber infrastructure and technologies”

for active demand management and wide-area monitoring and control, response to and managing cyber events, and risk/security assessments.

CURRENT LEGISLATION

Several bills introduced in the 112th Congress addressing the cybersecurity of the Smart Grid are summarized below.

Senate

The Cyber Security and American Cyber Competitiveness Act of 2011⁷⁴ (S. 21) would secure the United States against cyberattack and protect sensitive information and the identities of U.S. citizens and business. The bill focuses on the increasing dependence of the United States on information technology, and highlights a growing need for public awareness and preparedness of cyber-threats.

The Cybersecurity and Internet Freedom Act of 2011⁷⁵ (S. 413) is intended to enhance the “security and resiliency of the cyber and communications infrastructure” of the United States. Among its provisions, the bill would establish within DHS a National Center for Cybersecurity and Communications (NCCC) to protect the federal and national information infrastructure. The duties of the NCCC Director would include the identification and evaluation of cyber-risks to critical infrastructure (covered by the bill) on a continuous, sector-by-sector basis. The NCCC would also issue regulations establishing risk-based security performance requirements to secure covered critical infrastructure against cyber risks. Each owner or operator of covered critical infrastructure would be required to certify to the NCCC Director that approved security and emergency measures had been implemented. Civil penalties for non-compliance would be established by the bill. The President would be authorized by the bill to declare a national cyber-emergency, and would be required to notify owners and operators of critical infrastructure about the nature of a cyber-threat if a national cyber-emergency was declared.

The Cyber Security Public Awareness Act of 2011⁷⁶ (S. 813) is intended to promote the awareness of cybersecurity. Among its provisions, the bill requires a report from be DHS on technical options to enhance the security of information networks of entities which own or manage critical infrastructure.

The bill also requires a report from the Secretary of Homeland Security in consultation with the Secretary of Defense and the National Intelligence Director concerning the threat posed by a cyberattack to disrupt the national electrical grid and its implications to national security, the options for quick recovery to provide for national security as well as for restoration of all electrical service in the United States, and the development of a plan to prevent disruption of the U.S. grid by a cyberattack.

House

The National Infrastructure Development Bank Act of 2011⁷⁷ (H.R. 402) aims to facilitate infrastructure development. The bill identifies the nation's energy infrastructure as an area in need of modernization. Eligibility is extended to Smart Grid projects as energy infrastructure development.

The Secure High-voltage Infrastructure for Electricity from Lethal Damage Act⁷⁸ (H.R. 668) seeks to protect the bulk power system and electric infrastructure critical to the defense and wellbeing of the United States from EMP threats (such as nuclear weapons), or natural geomagnetic disturbance (GMD) vulnerabilities (such as solar flares). The bill proposes to authorize FERC to order the ERO to take emergency measures to protect the reliability of the bulk power system upon identification of an imminent threat to grid security from an EMP attack or GMD event. FERC would be authorized to allow utilities to recover "substantial costs" incurred from compliance with such an emergency order. The bill would also authorize FERC to issue rules or orders to protect against such grid security vulnerabilities not covered by ERO reliability standards (and would rescind the FERC rule or order when a sufficient ERO reliability standard was in place). FERC would be required to direct the ERO to propose reliability standards to protect against "reasonably foreseeable" EMP or GMD events. The ERO would also be required to propose reliability standards (balancing risks and costs) to address availability of large transformers capable of restoring reliable grid operations after an EMP or GMD event, providing entities (either individually or jointly) which own such transformers to ensure their adequate availability in case such transformers are destroyed or disabled by such an EMP or GMD event. The President would be required to identify up to 100 electric infrastructure facilities critical in supplying power for the defense of the United States which would be subject to FERC rules and orders related to EMP or GMD events. Recovery of full incremental costs incurred in compliance with such FERC

rules and orders would be allowed for owners of the identified defense critical electric facilities.

White House Legislative Proposal on Cyberspace

The Obama administration has launched its own comprehensive proposals for legislation on cybersecurity.⁷⁹ Protection of critical infrastructure (including the electric grid, financial systems, and transportation networks) is among the main proposals. Other initiatives are suggested to better report cyber-breaches so that consumers are aware that their personal data may have been accessed by intruders, and “synchronized” penalties for cyber-crime with mandatory minimum punishments for cyber-intrusions into critical infrastructure.

The Administration wants better preparedness and coordination between federal agencies, state governments, and industry in order to prevent cyberattacks against critical infrastructure. The proposals include development of cybersecurity standards and enhanced information sharing about cyber threats. The Administration also proposes legislative provisions for DHS to help industry, states, and local government to recover from a cyber-intrusion and fix the resulting damage, or provide advice on building a better network. DHS would also review cyber-protection strategies and requirements, making public its findings on readiness (while not revealing the specific nature of any deficiencies).

ADDITIONAL COMMENTS

Much of the federal efforts related to the cybersecurity of the smarter grid relate to efforts to stay ahead of cyber-threats. But such is the complexity of the cyber-threat universe (with defined threats, perceived weaknesses, and the possibility of continual upgrades of both hardware and software systems) that staying ahead of the threats could quickly evolve into a rapidly growing, never-ending cost center for utilities. While a key to cost control is in assessment of the likely risks, cost recovery for reliability under current federal law is based on mandatory compliance with CIP cybersecurity standards for reliability purposes.

Cost recovery for Smart Grid expenditures or upgrades is voluntary under current law. Such discretionary treatment may possibly result in liability

claims if damages result from an attack on Smart Grid systems. While the “Support Anti-Terrorism by Fostering Effective Technologies Act” of 2002⁸⁰ provides “risk management” and “litigation management” protection for qualified antiterrorism technologies and others in the supply and distribution chain, such protections likely do not apply to electric utilities as adopters of Smart Grid technologies and devices.

Current legislative and Administration proposals largely speak to a prioritization of critical infrastructure facilities, with consideration to how these relate to national security, and national economic recovery. However, recoverability from a cyberattack on the scale of something which might take down a significant portion of the grid will likely be very difficult. Maintaining a ready inventory of critical spare parts in close proximity to key installations would likely prove useful to quickening recovery efforts from some types of attack.

The current Smart Grid cybersecurity discussions largely focuses on the security of central station power plants and transmission systems. However, the future Smart Grid may increasingly depend on renewable energy, fuel cells, and other distributed resources like energy storage as these technologies are increasingly integrated into the nation’s energy framework. The development of the Smart Grid with distributed and renewable power generation resources may add a level of security to the grid, since these resources do not have the fuel requirements of fossil generation. Damage to the fossil fuel delivery networks would likely impair operation of central station generating plants, depending on how much of an inventory of fuel is stored on-site. This greater diversity of resource options would likely further enhance the Smart Grid’s expected improvement in reliability due a greater diversity of resource options, joining together these newer elements with traditional power stations in the power grid of the future. But the characteristics that these elements bring to the system could be considered in the design of CIP standards and protocols.

Although this report has focused on cybersecurity aspects of a smarter electrical grid, technologies being developed for use by the Smart Grid could also be used by natural gas pipeline, water supply, and telecommunications systems. Consideration could be given to applying similar control system device and system safeguards to these other vital utility systems. Consideration could be given to applying similar control system device and system safeguards to these other vital utility systems. The electricity grid is connected to (and largely dependent on) these other resource and communications providers as the vast majority of power production today

needs water for steam generation or natural gas for fuel. Similarly, natural gas pipelines use many electrically powered compressors to maintain pipeline pressure and move gas through the system, and the nation's water systems is a notable consumer of electricity for distribution and supply purposes. These interdependent systems are also vulnerable to natural hazards such as earthquakes and tornadoes. The remote sensing and other technologies expected to be employed by the Smart Grid could also help mitigate the effects of regional natural disasters on critical infrastructure, as these are expected to be capable of detecting outages and optimizing power flows to minimize damage and enable a more complete recovery.

End Notes

¹ EIA, Glossary, <http://www.eia.gov/tools/glossary/index.cfm?id=B>.

² EIA, Glossary, <http://www.eia.gov/tools/glossary/index.cfm?id=B>.

³ As of 2007, there were 210 investor-owned electric utilities, 2,009 publicly-owned electric utilities, 883 consumer-owned rural electric cooperatives, and nine federal electric utilities. Energy Information Administration (EIA), Electric Power Industry Overview 2007, <http://www.eia.doe.gov/electricity/page/prim2/toc2.html>.

⁴ The bulk power system makes it possible for utilities to engage in wholesale (sales for resale) electric power trade. U.S. Energy Information Administration, Overview—Power Transactions & Interconnected Networks, 2011, <http://www.eia.gov/cneaf/electricity/page/prim2/chapter7.html>.

⁵ Massachusetts Institute of Technology, Retrofitting of Coal-Fired Power Plants for CO₂ Emissions Reductions, March 23, 2009, <http://web.mit.edu/mitei/docs/reports/meeting-report.pdf>.

⁶ Thomas A. Prevost and David J. Woodcock, Transformer Fleet Health and Risk Assessment, Weidman Electrical Technology, IEEE PES Transformers Committee Tutorial, March 13, 2007, http://grouper.ieee.org/groups/transformers/info/S07/S07-TR_LifeExtension.pdf.

⁷ K. Anderson, D. Furey, and K. Omar, Frayed Wires: U.S. Transmission System Shows its Age, Fitch Ratings, October 25, 2006.

⁸ Key legislation include the Public Utility Regulatory Policies Act of 1978, the Energy Policy Acts of 1992 and 2005, and the Energy Independence and Security Act of 2007.

⁹ See Title XIII at 42 U.S.C. 17381 *et seq.*

¹⁰ CRS Report R41674, *Terrorist Use of the Internet: Information Operations in Cyberspace*, by Catherine A. Theohary and John Rollins.

¹¹ United States Department of Energy, Office of Electric Transmission and Distribution, "Grid 2030" *A National Vision for Electricity's Second 100 Years*, July 2003, p. 27, http://www.oe.energy.gov/DocumentsandMedia/Electric_Vision_Document.pdf.

¹² Pacific Northwest National Laboratory, *North American SynchroPhasor Initiative*, May 2011, <http://www.naspi.org/>.

¹³ U.S. Department of Energy, *Strategic Plan*, May 2011, http://www.energy.gov/news/documents/DOE_StrategicPlan.pdf.

- ¹⁴ “Demand Response” allows retail customers to participate in electricity markets by giving them the ability to respond to prices as they change over time—either daily or hourly in most instances. See <http://www.oe.energy.gov/demand.htm>.
- ¹⁵ The Eastern, Western and Texas interconnections of the U.S. grid. See http://www.eia.doe.gov/cneaf/electricity/chg_stru_update/fig7.html.
- ¹⁶ Critical Foundations: Protecting America’s Infrastructures, The President’s Commission on Critical Infrastructure Protection, October 1997, <http://www.fas.org/sgp/library/pccip.pdf>. (CF)
- ¹⁷ A system of remote control and telemetry used to monitor and control the transmission system. See <http://www.eia.doe.gov/tools/glossary/index.cfm?id=S>.
- ¹⁸ CF, p. 12.
- ¹⁹ The Smart Grid Interoperability Panel Cyber Security Working Group, Introduction to NISTIR 7628, National Institute of Standards and Technology, Guidelines for Smart Grid Cyber Security, September 2010, <http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf>. (NISTIR)
- ²⁰ NISTIR, p. 9.
- ²¹ Siobhan Gordon, Electricity Grid in U.S. Penetrated by Spies, The Wall Street Journal, April 8, 2009, <http://online.wsj.com/article/SB123914805204099085.html>.
- ²² Ibid.
- ²³ “[A worm is a]n independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.” See <http://www.gao.gov/new.items/d09661t.pdf>, p.6.
- ²⁴ “A successful attack by a software application such as the Stuxnet worm could result in manipulation of control system code to the point of inoperability or long-term damage. Should such an incident occur, recovery from the damage to the computer systems programmed to monitor and manage a facility and the physical equipment producing goods or services could be significantly delayed. Depending on the severity of the attack, the interconnected nature of the affected critical infrastructure facilities, and government preparation and response plans, entities and individuals relying on these facilities could be without life sustaining or comforting services for a long period of time. The resulting damage to the nation’s critical infrastructure could threaten many aspects of life, including the government’s ability to safeguard national security interests.” CRS Report R41524, The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability, by Paul K. Kerr, John Rollins, and Catherine A. Theohary.
- ²⁵ “The Stuxnet trojan/virus is the first publicly known ‘worm’ to target industrial control systems. The threat posed by Stuxnet has been portrayed as beyond anything seen before. Its goal was to sabotage a real-world industrial plant, not disrupt abstract IT systems. It was aimed at industrial control systems with the intention to reprogram PLCs [programmable logic controllers—devices used for control of processes] in a manner that would sabotage the plant, hiding the changes from programmers or users. Stuxnet has highlighted the potential to directly attack industrial control systems used in critical national infrastructure, including energy, water, and transport sectors.” Richard Piggins, Control Network Security Lessons from Stuxnet, Consulting-Specifying Engineer, February 3, 2011, http://m.csemag.com/index.php?id=2832&tx_ttnews%5Btt_news%5D=42715&cHash=42da992b88.
- ²⁶ Military Photos.net, AURORA Test Validated Fears of Dept. of Homeland Security, October 1, 2007, <http://www.militaryphotos.net/forums/showthread.php?121081-AURORA-test-validated-fears-of-Dept.-of-Homeland-Security>.

- ²⁷ U.S. Government Accountability Office, INFORMATION SECURITY Cyber Threats and Vulnerabilities Place Federal Systems at Risk, GAO-09-661T, May 5, 2009, p. 12, <http://www.gao.gov/new.items/d09661t.pdf>.
- ²⁸ Jeffrey Carr, “Ember Needs a Wake-Up Call from the CIA,” *Forbes*, January 31, 2011, <http://blogs.forbes.com/jeffreycarr/2011/01/31/ember-needs-a-wake-up-call-from-the-cia/>.
- ²⁹ A method of attack that denies system access to legitimate users without actually having to compromise the targeted system. From a single source, the attack overwhelms the target computers with messages and blocks legitimate traffic. It can prevent one system from being able to exchange data with other systems or prevent the system from using the Internet. See <http://www.gao.gov/new.items/d09661t.pdf>, p.5.
- ³⁰ A high-tech scam that frequently uses spam or pop-up messages to deceive people into disclosing sensitive information. Internet scammers use e-mail bait to “phish” for passwords and financial information from the sea of internet users. See <http://www.gao.gov/new.items/d09661t.pdf>, p. 6.
- ³¹ NISTIR. Page 7.
- ³² James St. Pierre, *Smart Grid Interoperability Panel Cyber Security Working Group*, National Institute of Standards and Technology, Presentation at National Electricity Forum, Washington, DC, February 16-17, 2011, p. 10, http://www.nationalelectricityforum.org/pdfs/NationalElectricityForum_StPierre_2011Feb08.pdf.
- ³³ Edison Electric Institute, *Spare Transformers*, 2011, <http://www.eei.org/ourissues/ElectricityTransmission/Pages/SpareTransformers.aspx>.
- ³⁴ Software that is embedded in a hardware device that allows reading and executing the software, but does not allow modification, e.g., writing or deleting data by an end user. See http://www.its.bldrdoc.gov/fs-1037/dir-015/_2236.htm.
- ³⁵ Committee on the Societal and Economic Impacts of Severe Space Weather Events, National Research Council, *Severe Space Weather Events—Understanding Societal and Economic Impacts: A Workshop Report*, National Academies, May 22-23, 2008, http://books.nap.edu/catalog.php?record_id=12507.
- ³⁶ *Ibid.*
- ³⁷ Yousaf M. Butt, “The EMP Threat: Fact, Fiction, and Response,” *Space Review*, February 1, 2010, <http://www.thespacereview.com/article/1553/2>.
- ³⁸ 18 U.S.C. § 1030.
- ³⁹ Interoperability can be defined as the capability of two or more networks, systems, devices, applications, or components to share and readily use information securely and effectively with little or no inconvenience to the user. GridWise Architecture Council, *Interoperability Path Forward Whitepaper*, November 30, 2005, http://www.gridwiseac.org/pdfs/interoperability_path_whitepaper_v1_0.pdf.
- ⁴⁰ The electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. http://www.nerc.com/files/Glossary_2009April20.pdf.
- ⁴¹ North American Electric Reliability Corporation, Rules of Procedure, March 21, 2008, http://www.nerc.com/files/NERC_Rules_of_Procedure_EFFECTIVE_20080321.pdf.
- ⁴² The maximum civil penalty which can be assessed for violation of reliability standards is \$1 million per day. Revised Policy Statement on Penalty Guidelines, 132 FERC ¶ 61,216, issued September 17, 2010.
- ⁴³ North American Electric Reliability Corporation, Reliability Standards for the Bulk Electric Systems of North America, April 20, 2010, http://www.nerc.com/files/Reliability_Standards_Complete_Set.pdf.

-
- ⁴⁴ Programmable electronic devices and communication networks including hardware, software, and data. http://www.nerc.com/files/Glossary_2009April20.pdf.
- ⁴⁵ In FERC Order No. 743, the North American Electric Reliability Corporation was directed to revise its definition of the term “bulk electric system” to ensure that the definition encompasses all facilities necessary for operating an interconnected electric transmission network. The revision will be made in accordance with NERC’s Reliability Standards development process. See <http://www.ferc.gov/whats-new/comm-meet/2010/111810/E-2.pdf>.
- ⁴⁶ The standards produced by the International Electrotechnical Commission (IEC) focus on the informational models and procedures necessary to promote the reliable and efficient operation of the Smart Grid. Standard IEC 62351 specifically addresses the cyber security of communications protocols.
- ⁴⁷ Federal Energy Regulatory Commission, Smart Grid Interoperability Standards—Supplemental Notice Requesting Comments, February 16, 2011, <http://www.ferc.gov/EventCalendar/Files/20110228084004-supplemental-notice.pdf>.
- ⁴⁸ U.S. Government Accountability Office, Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed, GAO-11-117, January 12, 2011, <http://www.gao.gov/products/GAO-11-117>.
- ⁴⁹ *Ibid.*, p. 27.
- ⁵⁰ Federal Energy Regulatory Commission, Letter from FERC Chairman Wellinghoff to David A. Pownier, Director, Information Technology Management Issues for the United States Government Accountability Office, December 23, 2010, <http://www.ferc.gov/industries/electric/indus-act/smart-grid/wellinghoff-response-GAO.pdf>.
- ⁵¹ Letter from G. Arnold, NIST to FERC Chairman J. Wellinghoff, dated April 7, 2011. See http://www.nist.gov/smartgrid/upload/FERC_Letter1.pdf.
- ⁵² U.S. Department of Energy, Office of Inspector General, Audit Report, Federal Energy Regulatory Commission’s Monitoring of Power Grid Cyber Security, January 2011, <http://www.ig.energy.gov/documents/IG-0846.pdf>. (DOEIG).
- ⁵³ DOEIG, pages 11-12.
- ⁵⁴ DOEIG, pages 21-22.
- ⁵⁵ Defined by NERC as “facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the bulk electric system.” See http://www.nerc.com/files/Glossary_of_Terms_2011Mar15.pdf.
- ⁵⁶ NERC works with eight regional entities to improve the reliability of the bulk power system. The members of the regional entities come from all segments of the electric industry: investor-owned utilities; federal power agencies; rural electric cooperatives; state, municipal and provincial utilities; independent power producers; power marketers; and endues customers. These entities account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico. See <http://www.nerc.com/page.php?cid=1%7C9%7C119>.
- ⁵⁷ U.S. Department of Energy Office of Electricity Delivery and Energy Reliability, Study of Security Attributes of Smart Grid Systems—Current Cyber Security Issues, INL/EXT-09-15500, April 2009, http://www.inl.gov/scada/publications/d/securing_the_smart_grid_current_issues.pdf.
- ⁵⁸ National Institute of Standards and Technology, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, NIST Special Publication 1108, January 2010, http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

- ⁵⁹ On July 16, 2009, the Commission issued a Smart Grid Policy Statement in which, among other things, the Commission explained its view that EISA does not make any Smart Grid standards mandatory and does not give the Commission authority to make or enforce any such standards. The Commission clarified that, under current law, its authority, if any, to make Smart Grid standards mandatory [or allow recovery in rates] derives from the Federal Power Act. Smart Grid Policy, 128 FERC ¶ 61,060, issued July 16, 2009. See <http://www.ferc.gov/whats-new/comm-meet/2009/071609/E-3.pdf>. (FERCSCP)
- ⁶⁰ The Commission also proposed to permit applicants to seek recovery of the otherwise stranded costs of legacy systems that are to be replaced by smart grid equipment. The Commission stated that an appropriate plan for the staged deployment of smart grid equipment, which could include appropriate upgrades to legacy systems where technically feasible and cost-effective, could help minimize the stranding of unamortized costs of legacy systems. The Commission therefore proposed that any request to recover stranded legacy system costs must demonstrate that such a migration plan has been developed. FERCSCP. Page 82.
- ⁶¹ Department of Homeland Security, Safeguard and Secure Cyberspace, http://www.dhs.gov/about/gc_1240609042614.shtm.
- ⁶² Federal Energy Regulatory Commission, FY 2010 Performance and Accountability Report, November 2010, <http://www.ferc.gov/about/strat-docs/2010-audit.pdf>.
- ⁶³ See footnote 58.
- ⁶⁴ FERCSCP, p. 27.
- ⁶⁵ M. D. Garratt, Distributech Highlights Challenge of SmartGrid: What's in it for Consumers?, CleanMakesGreen.com, February 7, 2011, <http://cleanmakesgreen.com/2011/02/07/distributech-highlights-challengeof-smartgrid-what%E2%80%99s-in-it-for-consumers/>.
- ⁶⁶ Business Wire, Smart Grid Cyber Security Market to Reach \$3.7 Billion by 2015, According to Pike Research, Smart Grid Cyber Security, June 23, 2010, http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news_view&newsId=20100623005613&newsLang=en.
- ⁶⁷ Mathew J. Schwartz, California Proposes Smart Grid Data Privacy Standards, Information Week, May 18, 2011, <http://mobile.informationweek.com/10247/show/8d96dc971db09af9557e4ad59b4708df&t=f6de813a074007af2879af82d46659ef>.
- ⁶⁸ Sherry Lichtenberg, Smart Grid Data: Must There Be Conflict Between Energy Management and Consumer Privacy?, National Regulatory Research Institute, December 2010, http://www.nrri.org/pubs/telecommunications/NRRI_smart_grid_privacy_dec10-17.pdf.
- ⁶⁹ Patricia Hoffman, Statement Before the U.S. Senate Committee on Energy and Natural Resources, Office of Electricity Delivery and Energy Reliability - U.S. Department of Energy, Cybersecurity of the bulk-power system and electric infrastructure, May 5, 2011, p. 5, http://energy.senate.gov/public/_files/HoffmanTestimony050511.pdf.
- ⁷⁰ See http://www.eei.org/ourissues/ElectricityTransmission/Documents/cyber_security_principles.pdf.
- ⁷¹ Electric Light & Power.com, DOE Picks EPRI Collaborative to Lead Cybersecurity Project, December 27, 2010, http://www.elp.com/index/display/article-display/6433556709/articles/electric-light-power/policy-and-regulation/2010/09/DOE_picks_EPRI_collaborative_to_lead_cybersecurity_project.html.
- ⁷² U.S. Department of Energy, Federal Smart Grid Task Force, http://www.oe.energy.gov/smartgrid_taskforce.htm.
- ⁷³ Trustworthy Cyber Infrastructure for the Power Grid, About TCIPG, 2011, <http://tcipg.org/about-tcipg-trustworthy-cyber-infrastructure-power-grid>.
- ⁷⁴ Introduced in January 2011 by Sen. Reid et al.

⁷⁵ Introduced in February 2011 by Sen. Lieberman et al.

⁷⁶ Introduced in April 2011 by Senators Whitehouse and Kyl.

⁷⁷ Introduced in January 2011 by Rep. DeLauro et al.

⁷⁸ Introduced in February 2011 by Rep. Franks et al.

⁷⁹ White House, Office of the Press Secretary, *Fact Sheet: Cybersecurity Legislative Proposal*, May 12, 2011, <http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal>.

⁸⁰ P.L. 107-296.

Chapter 3

CYBERSECURITY ISSUES FOR THE BULK POWER SYSTEM*

Richard J. Campbell

SUMMARY

In the United States, it is generally taken for granted that the electricity needed to power the U.S. economy is available on demand and will always be available to power our machines and devices. However, in recent years, new threats have materialized as new vulnerabilities have come to light, and a number of major concerns have emerged about the resilience and security of the nation's electric power system. In particular, the cybersecurity of the electricity grid has been a focus of recent efforts to protect the integrity of the electric power system.

The increasing frequency of cyber intrusions on industrial control (IC) systems of critical infrastructure continues to be a concern to the electric power sector. Power production and flows on the nation's electricity grid are controlled remotely by a number of IC technologies. The National Security Agency (NSA) reported that it has seen intrusions into IC systems by entities with the apparent technical capability "to take down control systems that operate U.S. power grids, water systems and other critical infrastructure."

As the grid is modernized and the Smart Grid is deployed, new intelligent technologies utilizing two-way communications and other

* This is an edited, reformatted and augmented version of a Congressional Research Service publication, No. R43989, dated June 10, 2015.

digital advantages are being optimized by Internet connectivity. Modernization of many IC systems (in particular, the Supervisory Control and Data Acquisition [SCADA] system) also has resulted in connections to the Internet. While these advances will improve the efficiency and performance of the grid, they also will increase its vulnerability to potential cyberattacks. *Black Energy*, *Havex*, and *Sandworm* are all recent examples of malware targeting SCADA systems. New devices (like smart meters) and increasing points of access (such as renewable electricity facilities) introduce new additional areas through which a potential cyberattack may be launched at the grid.

Many cybersecurity actions are reactive to the last threat discovered. While intrusion detection is a priority, some experts say that mitigation of cyber threats requires a focus on attackers, not the attacks. Cybersecurity strategies may shift from figuring out whether a system has been compromised to an understanding of who authored the malicious software and why. Although malware intrusions may not have resulted in a significant disruption of grid operations so far, they still have been possible even with mandatory standards in place. The North American Electric Reliability Corporation's (NERC's) current set of standards, Critical Infrastructure Protection (CIP) Version 5, is moving toward active consideration of bulk electric system security needs rather than just compliance with minimum standards.

Electric utilities emphasize the need for timely information sharing and advocate for liability protection from potential damages resulting from a major cyber event. Some observers argue that it is the responsibility of electric utilities to embrace security as part of their strategic business planning and operations. The National Electric Sector Cybersecurity Organization has identified six failure scenario domains intended to assist utility cybersecurity efforts. These scenarios also illustrate the continuing vulnerability of the grid to potential cyber and physical attacks, or a combination of both.

This report highlights several areas for congressional consideration to improve grid cybersecurity. One issue is whether electric utilities have the resources to make the financial investment and recruit staff to reduce vulnerabilities. Another issue is that NERC CIP standards do not apply to all points of grid connection to the distribution system, and these connections still may represent cyber vulnerabilities. The adequacy of current standards where they do apply is also an issue.

INTRODUCTION

In the United States, it is generally taken for granted that the electricity needed to power the U.S. economy is available on demand and will always be

available to power our machines and devices. However, in recent years, new threats have materialized as new vulnerabilities have come to light, and a number of major concerns have emerged about the resilience and security of the nation's electric power system. In particular, the cybersecurity¹ of the electricity grid has been a focus of recent efforts to protect the integrity of the electric power system.²

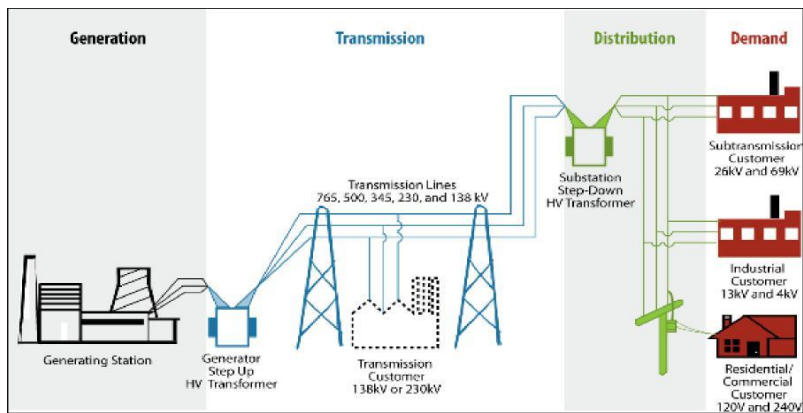
Power flows on the nation's electricity grid are remotely controlled by a combination of older, legacy systems and newer control technologies. Many of these legacy technologies are analog in design and were not originally connected to the Internet³ (although many are equipped with radio or other communications capabilities). But as the grid is modernized, the new "intelligent" technologies replacing them use advanced two-way communications and other digital advantages that likely will be optimized by Internet connectivity. While these advances will improve the efficiency and performance of the grid, they also potentially increase the vulnerability of the grid to cyberattacks.

Cybersecurity is today, and will continue to be, a major issue and focus area for the electric power sector. The energy sector (i.e., electricity, natural gas, and petroleum) is one of 16 critical infrastructure sectors designated by the Department of Homeland Security.⁴ Incidents of reported cyber intrusions and attacks aimed at undermining the U.S. grid appear to be increasing.⁵ While parts of the electric power subsector have mandatory and enforceable cyber and physical security standards,⁶ some have argued that minimum, consensus-based standards are not enough to secure the system.⁷ Further, the electric grid is not isolated from attacks on other critical infrastructure sectors on which it depends (i.e., the natural gas subsector, water, and transportation), and mandatory and enforceable cybersecurity standards apply to only a few of the 16 critical infrastructure sectors.⁸

This report will discuss the current state of electric sector cybersecurity, surveying existing regulations and proposed efforts to improve cybersecurity in the wake of recently reported threats and potential vulnerabilities. The report will focus on the bulk power system⁹ under authority of the Federal Energy Regulatory Commission (FERC), which Congress directed to establish mandatory and enforceable reliability standards.¹⁰ Many cybersecurity standards and actions are in response to cyber events. As such, basic compliance with standards by electric utility companies may not be enough to achieve effective cybersecurity protections. Areas for possible further congressional consideration or action will be highlighted in this report.

GRID COMPONENTS AND POTENTIAL VULNERABILITIES

The electric utility business encompasses the process of generating electricity and sending power to the ultimate user. The electrical grid is the name given to the machinery and power lines that enable power to be sent from the power plant to the ultimate user of electricity. As seen in **Figure 1**, this generally requires an infrastructure made up of generating stations (where the power is produced), step-up transformers and transmission lines (whereby transformers increase the voltage so that the electricity can be sent over very long distances), and step-down transformers and distribution lines (whereby the voltage can be lowered allowing the electricity to be sent to businesses and homes to power machinery and devices). Depending on the regulatory regime in place, these system elements may be controlled by companies under state jurisdiction or entities under federal jurisdiction (such as regional transmission organizations or federal power marketing administrations).



Source: Congressional Research Service, based on graphic found at <https://reports.energy.gov/BlackoutFinalWeb.pdf> (p. 5).

Note: kV = kilovolts (or 1,000 volts).

Figure 1. Electric Power System Elements.

Controlling and monitoring the various parts of the grid are industrial control (IC) systems, some of which are connected to the Internet. Other IC systems are not Internet-connected, and still rely on local area networks (LANs) or similar systems for control and reporting. The following paragraphs discuss these IC systems and potential vulnerabilities to intrusion and cyberattack.

Electric Utility Industrial Control Systems

The grid relies on a number of electronic devices, switches and circuit breakers to regulate and report on the flow of electricity at different parts of the system. Together, these pieces of mechanical and automated equipment constitute the grid's IC systems, managing power plant controls, transformer yard and power bus¹¹ functions, transmission system, and distribution substations.

The IC system essentially operates in a "control loop" in which sensors continually check key components, with variable responses against control variables in order to ensure that the system is functioning as designed. If responses show a disturbance resulting in operation of the system outside normal operating parameters, then the system adjusts actuators to bring the system back to process norms, or sends alerts to human-machine interfaces¹² (HMIs) to reconfigure the system or adjust operations in the control algorithms. Diagnostics and maintenance utilities are built into the system to "prevent, identify and recover from abnormal operation or failures."¹³

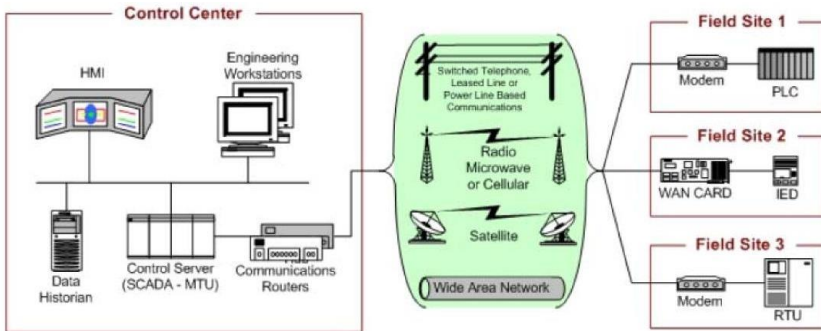
Supervisory Control and Data Acquisition Systems

One IC system used to control remote operations of the power grid is the Supervisory Control and Data Acquisition (SCADA) system.

SCADA systems are highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square kilometers, where centralized data acquisition and control are critical to system operation ... A SCADA control center performs centralized monitoring and control for field sites over long-distance communications networks, including monitoring alarms and processing status data. Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices. Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.¹⁴

SCADA systems have been in use at least since the 1970s, and were adopted at a time when the focus of system design was on function and reliability. An example of a basic SCADA network is shown in **Figure 2**. Historically, these systems consisted of remote terminal units¹⁵ which were

often connected to a mainframe computer via telephone lines or radio connections. They were not typically connected to centralized networks. Utilities typically operated separate control systems created just to operate power plants and related infrastructure.¹⁶



Source: See *Guide to Industrial Control Systems Security* at <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>.

Notes: WAN = Wide Area Network; MTU = Master Terminal Unit (server for SCADA system); IED = Intelligent Electronic Device; RTU = Remote Terminal Unit.

Figure 2. SCADA System General Layout.

Over time, modification of SCADA systems has resulted in connection of many of these older, legacy systems to the Internet. However, many of these legacy SCADA systems were not designed with security features, allowing other potential pathways for a cyberattack.¹⁷ As a result, these systems may be vulnerable to intrusion through data reporting pathways, or attacks (for example) using a thumb drive to download malware like the Stuxnet worm.¹⁸ However, some of these earlier designs and configurations may not be as vulnerable to an Internet-launched cyberattack. The security issue, for old and new systems, then becomes both how they are connected to the utility's other systems, and what levels of security exist to detect and deter potential intrusions.

Distributed Control Systems

Distributed control systems (DCSs) are used in power plant settings where process control requires feedback to maintain process conditions automatically about a desired set point. DCSs generally use several Programmable Logic Controllers (PLCs) to establish process tolerances. PLCs are typically

microprocessor- or computer-based devices that are used extensively to control industrial equipment or processes. Communications over DCS or PLC networks need to be more reliable and function at higher speeds “compared to the long-distance communication systems used by SCADA systems” because of the process control functions of DCSs.¹⁹

Modernization and the Smart Grid

The electric grid of the United States has been called an “engineering marvel,” but it is a system which in many places is becoming an “aging marvel.”

America relies on an aging electrical grid and pipeline distribution systems, some of which originated in the 1880s. Investment in power transmission has increased since 2005, but ongoing permitting issues, weather events, and limited maintenance have contributed to an increasing number of failures and power interruptions. While demand for electricity has remained level, the availability of energy in the form of electricity, natural gas, and oil will become a greater challenge after 2020 as the population increases. Although about 17,000 miles of additional high-voltage transmission lines and significant oil and gas pipelines are planned over the next five years, permitting and siting issues threaten their completion.²⁰

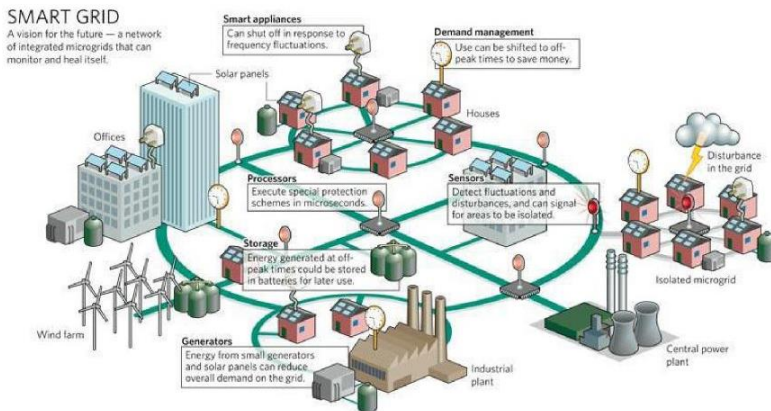
In recognition of the need to deploy new technologies, Congress indicated its support for grid modernization in the Energy Independence and Security Act of 2007 (EISA) (P.L. 110-140). Specifically, Section 1301 of the act states:

It is the policy of the United States to support the modernization of the Nation’s electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth ... which together characterize a Smart Grid...

The “Smart Grid” refers to the evolving electric power network as new information technology (IT) systems and communications capabilities are incorporated. EISA Section 1301 further states that aspects characterizing a Smart Grid include

- Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.
- Dynamic optimization of grid operations and resources, with full cybersecurity.
- Deployment of “smart” technologies (real-time, automated, interactive technologies that optimize the physical operation of appliances and consumer devices) for metering, communications concerning grid operations and status, and distribution automation.

Figure 3 provides a conceptual illustration of what a Smart Grid network may look like. The many disparate elements and user systems also emphasize the need for secure communications pathways required for Smart Grid operation.



Source: Consumer Energy Report. See <http://www.consumerenergyreport.com/wp-content/uploads/2010/04/smartgrid.jpg>.

Figure 3. Concept of a Smart Grid Network.

Smart Grid networks are also potentially better able to integrate the intermittent energy from renewable electricity technologies (i.e., renewable electricity systems such as distributed solar photovoltaic [PV] and wind), distributed generation, demand response, and consumer energy efficiency programs.²¹

While the potential of the Smart Grid to revolutionize the ways power is generated and used is great, so too are the potential cybersecurity risks.²² Additional Smart Grid components may add to the ability to control power flows and enhance the efficiency of grid operations, they also potentially

increase the susceptibility of the grid to cyberattack. Smart Grid components are built around microprocessor and other hardware devices whose basic functions are controlled by software programming. These devices and functions may be subject to manipulation over a network.²³ The information processing and communications attributes which make the Smart Grid attractive are the very same attributes which can increase the vulnerability of the electric power system and its critical infrastructure to a possible cyberattack. This risk is potentially increased for systems connected to the Internet.

Other Potential Vulnerabilities

The grid has other potential vulnerabilities and avenues that a cyberattacker might seek to exploit. Independent researchers are reported to have found hacking into grid computer networks to be “startlingly easy,” and they have alerted authorities to their findings.²⁴ While new security systems and controls are added to address known weaknesses, new vulnerabilities may emerge as new devices and avenues of access are added.

Distributed Generation

Renewable electricity generation is increasing and is highly distributed to capture the best renewable resources available to maximize the amount of power generated. However, these facilities can represent potential backdoors for cyberattackers to access the grid. Renewable electricity companies in Europe reportedly were targeted by cyberattackers at a clean power website from which malware was passed to visitors, thus giving the attackers access to the power grid:

The communication networks and software that link green energy sources to the grid as well as the electronic meters that send real time power usage to consumers and utilities are providing new back-door entry paths for computer hackers to raise havoc with the grid.²⁵

Smart Meters

Smart meters are an example of new systems added to the grid. While such systems are designed with security in mind (i.e., following international standards using best practices such as encryption of sensitive data, system protection from viruses and malware, access control and tamper alerts on

meters, and two-party authorization), systems analysts acknowledge that such connected systems can have new vulnerabilities.²⁶ Smart meters were singled out as a vulnerability by a report as potentially being susceptible to fraud from “manipulated meter readings, misuse of private customer data and a threat of power outages through a large cyberattack.”²⁷ One particular weakness was said to be the built-in encryption of data sent from smart meters to utilities. The meters are designed to last approximately 20 years, but it was speculated that the device’s built-in cryptology system may not be secure for that long a period.²⁸ However, another source says that smart meter encryption and authentication “should be readily and proactively updatable” and combined with intrusion detection to better protect networks.²⁹

Supply Chains

Supply chains are another potential vulnerability that affects old legacy systems as well as new Smart Grid hardware and software applications. Legacy systems are a particular concern because upgrades and repairs of equipment may not include installation of security upgrades. New procurement guidance for energy delivery systems focus on life cycle considerations by providing “baseline cybersecurity procurement language for use by asset owners, operators, integrators, and suppliers during the procurement process.”³⁰ Security of the supply chain for newer Smart Grid systems is a significant procurement concern because many components are obtained from many sources and vendors internationally. These sources may be considered targets of opportunity to compromise or counterfeit Smart Grid components.³¹

Supply chain best practices in security and resilience need to be benchmarked and shared with the power sector. These practices need to be explored and explained in dialogues between IT and supply chain professionals, and between utilities and their suppliers.³²

THE GRID IS EXPERIENCING CYBER INTRUSIONS

The increasing frequency of cyber intrusions on industrial control systems of critical infrastructure is a trend of concern to the electric utility industry. The National Security Agency reported that it has seen intrusions into IC systems by entities with the apparent technical capability “to take down control systems that operate U.S. power grids, water systems and other critical infrastructure.”³³ These intrusions, while they have not manifested in

cyberattacks capable of inhibiting or disrupting electric system operations, still have reportedly occurred with CIP mandatory standards in place. Some have asserted that consensus-based standards are not strong enough, or are not developed quickly enough, to address cybersecurity needs, while others believe the cost of meeting the standards goes beyond the perceived risks.³⁴

The following paragraphs describe several recently reported incidents of cyber intrusions and examples of malware³⁵ found on IC systems that are commonly used to control energy flows on the electric grid.

BlackEnergy

In October 2014, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) announced that several industrial control systems had been infected by a variant of a Trojan horse³⁶ malware program called BlackEnergy.³⁷ Originally designed for “nuisance spam³⁸ attacks,” the software for BlackEnergy was first reported in 2007 and is designed to target critical energy infrastructure.³⁹

BlackEnergy is a special concern for critical infrastructure companies because the software is being used in an Advanced Persistent Threat (APT)⁴⁰ form ostensibly to gather information.

BlackEnergy specifically targets human machine interface (“HMI”) software, which enables users to monitor and interact with industrial control systems such as heating, ventilation, and air conditioning systems through a dashboard or other type of graphical interface. HMI software is typically running 24/7, can be remotely accessed, and is rarely updated, thus making it a favorite target for opportunistic hackers.⁴¹

While no attempts to “damage, modify, or otherwise disrupt the victim systems’ control processes were found,” the ICS-CERT alert indicates that this APT variant of BlackEnergy is a special concern because it is a modular malware capable moving through network files onto removable storage media.

[T]ypical malware deployments have included modules that search out any network-connected file shares and removable media for additional lateral movement within the affected environment. The malware is highly modular and not all functionality is deployed to all victims.⁴²

Hackers are reported to have used the BlackEnergy Trojan horse to deliver plug-in modules used for several purposes, including keylogging, audio recording, and grabbing screenshots. Researchers looking at the BlackEnergy malware are reported to have identified a plug-in that can destroy hard disks, and believe that the attackers will activate the module once they are discovered in order to hide their presence.⁴³

HAVEX

The HAVEX malware is not new, but it has been modified several times since its first reported deployment. It has targeted the energy sector since “at least August 2012.”⁴⁴ Originally, HAVEX was distributed via spam email or spear-phishing attacks.⁴⁵ This new version of HAVEX appears to have been designed as a Trojan horse specifically to infiltrate and modify “legitimate” software from ICS and SCADA suppliers, adding an instruction to run code (i.e., the “*mbcheck.dll*” file) containing the HAVEX malware.⁴⁶

In the instance discovered, HAVEX malware was used as a remote access tool (RAT) to extract data from Outlook address books and ICS-related software files used for remote access from the infected computer to other industrial servers.⁴⁷ The cyberattack leaves the company’s system in what appears to be a normal operating condition, but the attacker now has a backdoor to access and possibly control the company’s ICS or SCADA operations.

The HAVEX malware possibly entered the control systems of targeted companies using one or multiple levels of attack:

- 1) Email Campaign: Executives and senior employees were targeted with malicious PDF attachments in February-June 2013.
- 2) Watering Hole Attack: Websites likely to be visited by people working in the energy sector were infected such that they redirected the site visitor to another compromised legitimate website hosting an exploit kit. The exploit kit then installs the RAT. This method of distribution began in June 2013.
- 3) Software Downloaded from ICS-Related Vendors: At least three ICS vendors’ software downloads were hacked so that they included the RAT malware.⁴⁸

HAVEX is also called “Backdoor.Oldrea” (or the “Energetic Bear RAT”), as it contains the malware known as “Kragany” or “Trojan.Kragany.” HAVEX is a product of the Dragonfly group (aka Energetic Bear), which appears to be

a “state-sponsored”⁴⁹ undertaking focused on espionage with sabotage as a “definite secondary capability.”⁵⁰ The malware allows attackers to upload and download files from the infected computer and run executable files. It was also reported to be capable of collecting passwords, taking screenshots and cataloguing documents.⁵¹

Sandworm

Sandworm is a type of Trojan horse, and it was originally focused on a vulnerability in the Windows operating system (reported as patched by Microsoft in October 2014).⁵² It was used to deliver malware through Powerpoint files on thumb drives using automatically run files, but that vector of attack has been largely closed.⁵³ The primary mode of Sandworm attack was spearphishing, using grammatically well-written emails with topics of interest to the target. The malware contained an attachment that exploited the vulnerability to deliver variants of the BlackEnergy Trojan.⁵⁴

The focus of the Sandworm attack discovered was SCADA systems, as the malware targeted specific software used for these systems.

On October 14th, a report was publicly released regarding the Sandworm team. After beginning an investigation into the affiliated malware samples and domains, we quickly came to realization that this group is very likely targeting SCADA-centric victims who are using GE Intelligent Platform’s CIMPLICITY HMI solution suite ... CIMPLICITY is an application suite that is used in conjunction with SCADA systems. A key component of any SCADA system is the HMI. The HMI (which stands for Human-Machine interface) can be viewed as an operator console that is used to monitor and control devices in an industrial environment.⁵⁵

Sandworm can potentially have greater impacts on an enterprise, as the malware could be transferred to other corporate business systems.

These devices can be responsible for automation control as well as safety operations... It is important to note that we are currently seeing CIMPLICITY being used as an attack vector; however, we have found no indication that this malware is manipulating any actual SCADA systems or data. Since HMIs are located in both the corporate and control networks, this attack could be used to target either network segment, or used to cross from the corporate to the control network.⁵⁶

MANDATORY BULK POWER CYBERSECURITY STANDARDS

The bulk electric power system⁵⁷ has mandatory and enforceable standards for cybersecurity. The Energy Policy Act of 2005 (EPACT) (P.L. 109-58) gave the Federal Energy Regulatory Commission authority over the reliability of the grid, with the power to approve mandatory cybersecurity standards proposed by the Electric Reliability Organization (ERO). Currently, the North American Electric Reliability Corporation (NERC) serves as the ERO. NERC therefore proposes reliability standards for critical infrastructure protection (CIP) which are updated considering the status of reliability and cybersecurity concerns for the grid.

FERC views grid security as a high priority, and separately established the Office of Energy Infrastructure Security (OEIS) to deal with cyber and physical security. OEIS has a mission to provide expertise to the Commission to “identify, communicate and seek comprehensive solutions to potential risks to FERC-jurisdictional facilities from cyberattacks and such physical threats as electromagnetic pulses.”⁵⁸ However, FERC still asserts that it does not have the authority to act quickly in the event of a major cyber event.⁵⁹

Defining the Extent of FERC’s Authority over Cybersecurity

NERC originally determined which electric industry facilities would be subject to mandatory reliability standards based on its definition of the term “bulk electric system” (BES). However, the regional bodies making up NERC had discretion in determining which facilities would be subject to these reliability standards under NERC’s guidelines for the definition.

FERC has authority over wholesale power sales and the transmission of electricity in interstate commerce, and it is responsible for the reliability of the bulk electric system.⁶⁰ States regulate electric distribution systems.⁶¹ FERC was concerned that certain facilities needed to ensure bulk power system reliability were not being considered under NERC’s definition of the bulk electric system. FERC acknowledged that EPACT excluded local distribution systems from its reliability mandate under Section 215 of the Federal Power Act, as not being part of the bulk power system.⁶² However, while that definition excluded facilities in Alaska and Hawaii, it also excluded virtually the entire grid in cities with large distribution systems like New York City.

In 2010, FERC directed NERC to develop uniform criteria for determining which facilities were necessary for the operation of the

“interconnected transmission network,” with the intention of including all such systems under NERC’s CIP regulations. FERC approved NERC’s revised criteria and new definition of the BES in 2012.⁶³ These criteria and definitions apply to all NERC regions and are a bright-line threshold including all Transmission Elements operated at 100 kilovolts (kV) or higher, and real power⁶⁴ and reactive power⁶⁵ resources connected at 100 kV or higher. This definition does not include facilities used in the local distribution of electric energy.

The revised definition of the BES allowed the potential inclusion of some facilities typically considered as distribution level, if they were seen as necessary for the operation of the interconnected transmission network. However, there are still many areas of potential access to the BES from the distribution system (which are not necessarily important to the operation of the transmission system), and thus beyond NERC’s CIP regulations and FERC’s reliability mandate. Because there are no mandatory standards of protection for distribution facilities below the bright-line threshold, these potentially “less protected” seams of the BES may provide a backdoor to cyber intrusions to the grid.⁶⁶

Toward a Focus on Security and Not Just Compliance

The current iteration of NERC’s standards is CIP Version 5,⁶⁷ which appears to be moving utility companies toward an active consideration of system security needs rather than just compliance with the standards. It is largely the result of concerns that some owner/operators were not designating their bulk electric power facilities as “critical cyber assets,” leaving potential “holes” in bulk electric power system cybersecurity.⁶⁸

The most notable change is the tiered impact rating system, which classifies bulk electric system (BES) Cyber Systems into High, Medium, and Low categories. This approach results in all cyber assets that could impact BES Facilities being in scope for the CIP standards ... Version 5’s tiered classification brings all BES generating facilities into scope for at least some requirements. Cyber assets meeting certain criteria will be grouped into systems and assigned a High, Medium, or Low impact rating based upon the characteristics of the facility they support. For example, BES Cyber Systems at plants larger than 1,500 MW may receive a Medium impact rating, while most black-start units will be Low

impact. All such systems, referred to officially as BES Cyber Systems, will be assigned at least a Low impact rating and will be required to comply with at least a portion of the requirements.⁶⁹

CIP Version 5 therefore establishes new criteria and requirements for bulk electric system (BES) Cyber Systems,⁷⁰ mandating compliance but requiring owner/operators of bulk electric systems to focus on improving the security of critical assets. BES assets, once categorized as low or high impact, must be protected according to the level of requirements for that impact category. Among other factors, CIP Version 5 now requires encryption of grid command and control signals; “role-based” instead of “risk-based” classifications requiring multiple levels of compliance considering facilities with low, medium or high-level impacts on the BES; monitoring and control of remote access Internet connections (with inclusion of serial connections); multiple-factor authentication (rather than a simple one-step password for access), incident response recovery plans; physical security of BES cyber assets to prevent unauthorized physical entry and access; and cataloging of all software and all security patches on BES devices.^{71, 72}

Among the concerns raised with the implementation of CIP Version 5 is the potentially high cost.⁷³ With the new BES designation, all facilities (whether these are low, medium, or high risk) will be covered by some level of the new requirements. Many of these facilities may not have been designated cyber assets before, so the costs of compliance likely will increase.

GOVERNMENT AND INDUSTRY COOPERATION ON GRID CYBERSECURITY

Cooperation between the federal government and the electric power sector now extends beyond mandatory and enforceable industry standards for the bulk electric system. However, such cooperation has not always been typical. Companies apparently were not aware of other government efforts. Reports began to emerge in 2010 that the federal government has been developing the capability to detect cyber intrusions on private critical infrastructure company networks. The program dubbed *Perfect Citizen* reportedly was designed to detect cyber intrusions using sensors in computer networks that would be activated by “unusual activity.”⁷⁴

While a number of voluntary structures now exist for information sharing and cybersecurity strategies, the degree of adoption by electric utilities and the overall effectiveness of these programs is unknown. The FY2016 budget proposes \$14 billion in cybersecurity funding for “critical initiatives and research” across the federal government.⁷⁵

Several of the key organizations and their missions with regard to electric power sector cybersecurity are profiled below.

Department of Energy

The Department of Energy (DOE) is home to a number of voluntary initiatives and programs for electric sector cybersecurity, with the Office of Electricity Delivery and Energy Reliability (OE) having the lead role. DOE considers the security and resilience of the electric sector to be paramount “... since it is arguably the most complex and critical infrastructure that other sectors depend upon to deliver essential services.”⁷⁶ Several of these programs are described below.

National Electric Sector Cybersecurity Organization (NESCO)

In 2009, under the FY2010 Energy and Water Appropriations Act (P.L. 111-85), Congress directed DOE to form a national organization which would serve as the National Electric Sector Cybersecurity Organization resource.

[T]he Secretary shall establish an independent national energy sector cyber security organization to institute research, development and deployment priorities, including policies and protocol to ensure the effective deployment of tested and validated technology and software controls to protect the bulk power electric grid and integration of smart grid technology to enhance the security of the electricity grid.⁷⁷

DOE selected two organizations to form the National Electric Sector Cybersecurity Organization (NESCO): EnergySec and the Electric Power Research Institute (EPRI).⁷⁸ EnergySec provides support for “information sharing, professional development and collaborative programs and projects that improve the cyber security posture of all participating organizations.” EPRI serves as the research and analysis resource for NESCO. NESCO’s mission is to improve the “cybersecurity posture of the electric sector by establishing a broad-based public-private partnership for collaboration and

cooperation” by providing a forum for cybersecurity experts, developers, and systems users.⁷⁹

Electricity Subsector Cybersecurity Capability Maturity Model

The Cybersecurity Capability Maturity Model (C2M2) was developed by DOE-OE, the Department of Homeland Security (DHS), and industry as a self-evaluation survey tool for any organization to address cybersecurity vulnerabilities. The C2M2 asks users to assess cybersecurity control implementation across 10 areas of cybersecurity “best practices” based on an evaluation of the maturity of a specific cybersecurity function.⁸⁰ The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) goes one step further, specifically tailoring the core C2M2 survey for the electricity subsector with a “maturity model, an evaluation tool, and DOE facilitated self-evaluations.”⁸¹

Additionally, in 2006, DOE released a report titled *Roadmap to Secure Control Systems in the Energy Sector*. It outlined a strategic framework to be developed by industry, vendors, academia and government stakeholders to “design, install, operate, and maintain a resilient energy delivery system capable of surviving a cyber-incident while sustaining critical functions.” The plan called for a 10-year implementation timeline focusing on barriers and recommended strategies for achieving effective grid cybersecurity. A five-year update released in 2011 highlighted what had been achieved to date, discussing ongoing efforts with respect to short- to long-term goals.⁸²

Department of Homeland Security

DHS has a broad mission to make the United States safe and resilient against terrorism and other potential threats.⁸³ The cyber and physical security of the grid are encompassed in this mission, and DHS has several initiatives in pursuit of these goals.

National Protection and Programs Directorate

The National Protection and Programs Directorate (NPPD) coordinates national efforts to protect critical infrastructure, working with partners “at all levels of government, and from the private and non-profit sectors” to share information to make critical infrastructure more secure. Under NPPD are several offices focused on cybersecurity, critical infrastructure protection, and resiliency.⁸⁴

- The Office of Cyber and Infrastructure Analysis (OCIA) uses information received from public and private sources to conduct consequence modeling, simulation, and analysis to inform cyber and physical security risk management for U.S. critical infrastructure.
- The Office of Infrastructure Protection (IP) helps critical infrastructure owners and operators to understand and address risks to critical infrastructure. The office provides tools and training to critical infrastructure owners to help them manage risks to their assets, systems, and networks.
- The Office of Cybersecurity and Communications (CS&C) is responsible for enhancing the security, resilience, and reliability of the nation's cyber and communications infrastructure. A major priority of the office is the reduction of cyber risks to federal and private Internet domains from terrorist attacks, natural disasters, or other emergencies. CS&C is also the home of the National Cybersecurity and Communications Integration Center (NCCIC).

NCCIC is focused on “cyber situational awareness, incident response, and management.”⁸⁵ NCCIC acts as an information sharing forum for the public and private to improve understanding of cybersecurity and communications vulnerabilities and incidents, and mitigation and recovery from cyber events. NCCIC's mission is to reduce the likelihood and severity of incidents that may “significantly compromise the security and resilience of the Nation's critical information technology and communications networks.”⁸⁶

The NCCIC works closely with those federal departments and agencies most responsible for securing the government's cyber and communications systems, and actively engages with private sector companies and institutions, state, local, tribal, and territorial governments, and international counterparts. Each group of stakeholders represents a community of practice, working together to protect the portions of critical information technology that they own, operate, manage, or interact with.⁸⁷

Two critical branches of NCCIC with functions important to electric grid cybersecurity are the United States Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

US-CERT brings advanced network and digital media analysis expertise to bear on malicious activity targeting our nation's networks. US-CERT develops timely and actionable information for distribution to federal departments and agencies, state and local governments, private sector organizations, and international partners. In addition, US-CERT operates the National Cybersecurity Protection System (NCPS), which provides intrusion detection and prevention capabilities to covered federal departments and agencies.⁸⁸

ICS-CERT reduces risk to the nation's critical infrastructure by strengthening control systems security through public-private partnerships. ICS-CERT has four focus areas: situational awareness for Critical Infrastructure and Key Resources stakeholders; control systems incident response and technical analysis; control systems vulnerability coordination; and strengthening cybersecurity partnerships with government departments and agencies.⁸⁹

US-CERT developed the Einstein 2 intrusion detection system used by the National Cybersecurity Protection System (NCPS).

NCPS intrusion detection capabilities alert DHS to the presence of malicious or potentially harmful computer network activity transiting to and from participating in federal executive branch civilian agencies' information technology networks. This capability is deployed via EINSTEIN 2 and provides for improved detection and notification capabilities to provide near real time response to cyber threats.⁹⁰

ICS-CERT coordinates responses to control systems-related security incidents and facilitates information sharing⁹¹ among federal, state, and local agencies and organizations; the intelligence community; and private sector constituents, including vendors, owners and operators, and international and private sector CERTs. The focus on control systems cybersecurity provides a direct path for coordination of activities among all members of the critical infrastructure stakeholder community.

Science and Technology Directorate

The Science and Technology Directorate (S&T) was created to provide science and technology in support of DHS's mission. Since DHS assists in efforts for the security and resiliency of the grid, the Smart Grid with characteristics of self-healing from power disturbance events, and operating resiliently against physical and cyber threats is of particular interest.⁹²

S&T also has a Cyber Security Division whose mission is to enhance the security and resilience of the nation's critical information infrastructure and the Internet by⁹³

- 1) developing and delivering new technologies, tools and techniques to enable the United States to defend, mitigate and secure current and future systems, networks and infrastructure against cyberattacks;
- 2) conducting and supporting technology transition; and
- 3) leading and coordinating cybersecurity research and development for department customers, and with government agencies, the private sector and international partners.

Since recovery from cyberattacks is seen as a part of S&T's resiliency focus, S&T is working on several electric power sector specific initiatives. These include the *Resilient Electric Grid* (an effort to "keep the lights on" in the event of a power outage by enabling distribution level power substations to share power with one another), and the *Recovery Transformer* (a program developing a prototype large power transformer to enable a quicker recovery [i.e., within days instead of months or years] from an event which might damage key transformers).⁹⁴ S&T is currently managing an effort to assess the state of the Smart Grid concept, as well as specific technologies needed to achieve goals of ensuring Smart Grid security and resiliency.⁹⁵

National Institute of Standards and Technology

The Energy Independence and Security Act of 2007 (EISA) (P.L. 110-140) defined attributes of a Smart Grid and plans for its development. EISA also gave the National Institute of Standards and Technology (NIST) the role of coordinating the development of a framework to enable the development of the Smart Grid in a safe and secure manner. Because cybersecurity threats were perceived as "diverse and evolving," NIST advocated a defense-in-depth strategy with multiple levels of security and asserted no single security measure could counter all types of threats.⁹⁶ The key to NIST's suggested approach is the determination of risk (i.e., the potential for an unwanted outcome resulting from internal or external factors, as determined from the likelihood of occurrence and the associated consequences) as quantified by the threat (e.g., event, actor or action with potential to do harm), the vulnerability

(e.g., weakness in the system), and the consequences (e.g., physical impacts) to the system.⁹⁷

NIST published its *Guidelines for Smart Grid Cybersecurity*⁹⁸ as a comprehensive, voluntary framework for organizations to use in developing effective cybersecurity strategies “tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities.”

According to NIST, deliberate attacks are not the only threat to Smart Grid cybersecurity.

Smart grid cybersecurity must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but also inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. The Smart Grid Interoperability Panel (SGIP) Cybersecurity Committee (SGCC) ... is moving forward in FY14 to address the critical cybersecurity needs in the areas of Advanced Metering Infrastructure security requirements, cloud computing, supply chain, and privacy recommendations related to emerging standards. This project will provide foundational cybersecurity guidance, cybersecurity reviews of standards and requirements, outreach, and foster collaborations in the cross-cutting issue of cybersecurity in the smart grid.⁹⁹

NIST established the Smart Grid Interoperability guidelines with a primary goal of developing a cybersecurity risk management strategy to enable secure “interoperability”¹⁰⁰ of technologies across different Smart Grid domains and components.

NIST was asked in 2013 by Presidential Executive Order No. 13636, “Improving Critical Infrastructure Cybersecurity,”¹⁰¹ to lead the development of a “Cybersecurity Framework” to reduce cyber risks.¹⁰² The framework was based on industry methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks, incorporating “voluntary consensus standards and industry best practices to the fullest extent possible.” The first version of the Framework was released on February 12, 2014.¹⁰³ Sector-specific federal agencies (such as DOE) are to report annually to the President on the extent to which owners and operators of critical infrastructure at greatest risk are participating in the program.¹⁰⁴

NIST also hosts the National Cybersecurity Center of Excellence, which is focused on getting better adoption of secure, commercially available cybersecurity technologies by both the public and private sectors.¹⁰⁵

North American Electric Reliability Corporation (NERC)

NERC's Critical Infrastructure Protection Committee (CIPC) is responsible for its physical security and cybersecurity initiatives. CIPC consists of both NERC-appointed regional representatives and technical subject matter experts, and serves as an expert advisory panel to the NERC Board of Trustees. It has standing subcommittees in the areas of physical security and cybersecurity. The CIPC also oversees the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).¹⁰⁶

Electricity Sector Information Sharing and Analysis Center (ES-ISAC)

ES-ISAC seeks to establish situational awareness, incident management, coordination and communication capabilities within the electricity sector through timely information sharing. The ES-ISAC works with DOE and the Electricity Sector Coordinating Council (ESCC) to share critical information with the electricity sector, enhancing its ability to "prepare for and respond to cyber and physical threats, vulnerabilities and incidents."¹⁰⁷

The Electricity Sector Information Sharing and Analysis Center ... which was established in 1998 under Presidential Decision Directive 63 (President Bill Clinton), called for the establishment of an ISAC for each of the eight infrastructure industries deemed critical to our national economy and public well-being.¹⁰⁸

NERC members who are "registered entities"¹⁰⁹ can report information regarding cyber incidents to ES-ISAC via a secure Internet exchange, and also receive information on threats.¹¹⁰

Electricity Sub-Sector Coordinating Council (ESCC)

The Electricity Sub-Sector Coordinating Council is the principal liaison between the federal government and the electric power sector. It represents the electricity sub-sector (as part of the Energy Critical Infrastructure sector)¹¹¹ under DHS's National Infrastructure Protection Plan (NIPP).¹¹² The ESCC draws its membership from all segments of the electric utility industry, and is led by three chief executive officers—one each from the American Public Power Association, the Edison Electric Institute, and the National Rural Electric Cooperative Association.¹¹³ Among its activities, the ESCC

coordinates industry and government efforts on grid security, guides infrastructure investments and R&D for critical infrastructure protection, seeks to improve threat information sharing and processes with public and private sector stakeholders, and coordinates cross sector activities with other critical infrastructure sectors. A Senior Executive Working Group (SEWG) supports the mission and activities of the ESCC, creating ad hoc “sub teams” to address goals identified by utility and government executives.¹¹⁴

Edison Electric Institute

The Edison Electric Institute (EEI) as the trade association for investor-owned electric utilities has been involved with the formation of industry partnerships on cybersecurity issues with a number of federal agencies. Information sharing between public and private entities is an issue the industry considers critical in protecting the grid against cyber-threats.¹¹⁵ The industry is involved in several information sharing efforts including the ES-ISAC, ESSC, and NCCIC.

EVALUATING AND IMPROVING ELECTRICITY SUBSECTOR CYBERSECURITY

As noted above, the bulk electric system has mandatory standards for critical infrastructure cybersecurity that NERC proposes, and FERC approves (or may modify and remand back to NERC). Industry compliance with these standards may be enough to prevent fines, but the question is whether existing mandatory standards result in a cybersecure grid. The grid has reportedly experienced intrusions to SCADA systems, which could possibly compromise systems operations. While the exact details and location have not been revealed, the cyberattacks demonstrate potential threats to grid reliability. Although some may believe the risks of a major cyberattack on the grid are small, FERC is obligated to consider CIP and cybersecurity as part of its reliability mandate. This section will summarize current concepts for evaluating and improving electricity subsector cybersecurity.

NESCO Cybersecurity Failure Scenarios

In 2013, NESCO released the results of an analysis intended to help electric utilities plan for cybersecurity risks. The “Electric Sector Failure Scenarios and Impact Analyses”¹¹⁶ report focuses on specific events in which the “failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or distribution of power.” The report organizes the failure scenarios according to six categories, corresponding to the domains identified by the National Institute of Standards and Technology.¹¹⁷

1. Advanced Metering Infrastructure (AMI)¹¹⁸
2. Distributed Energy Resources (DER)¹¹⁹
3. Wide Area Monitoring, Protection, and Control (WAMPAC)¹²⁰
4. Electric Transportation (ET)¹²¹
5. Demand Response (DR)¹²²
6. Distribution Grid Management (DGM)¹²³

A seventh, generic cross-cutting scenario was also identified which could impact any of these categories. The failure scenarios are “high-level” examples, so as not to present a cyberattacker with ideas on how to carry out an attack. The focus is on cybersecurity events, not other events which could potentially cause similar issues. Mitigations and options are suggested for the various scenarios, with a scheme for prioritization of solutions for securing control systems. The report was designed to “support risk assessment, policies, planning, procedures, procurement, training, tabletop exercises and security testing.”¹²⁴

Figure 4 lists what NESCO considered as some of the top potential failure scenarios. NESCO teams ranked the scenarios, with the darker bands indicating the potential higher risk failures. A relatively large number of potential failures came from the WAMPAC domain, a significant number from AMI, and a moderate number came from the DGM domain. Few were selected from DER or DR, and none were selected from the ET domain.

In the report, each failure scenario is accompanied by a descriptive example of an action causing the breach, the relevant vulnerabilities and impacts. A possible mitigation of the AMI.24 scenario above is shown in the example of **Figure 5**.

AMI.1	Authorized Employee Issues Invalid Mass Remote Disconnect
AMI.3	Invalid Access Used to Install Malware Enabling Remote Internet Control
AMI.23	Meter Authentication Credentials are Compromised and Posted on Internet
AMI.24	Weak Encryption Exposes AMI Device Communication
AMI.25	Known but Unpatched Vulnerability Exposes AMI Infrastructure
DER.1	Inadequate Access Control of DER Systems Causes Electrocution
DER.16	DER SCADA System Issues Invalid Commands
WAMPAC.1	Denial of Service Attack Impairs NTP Service
WAMPAC.2	Networking Equipment used to Spoof WAMPAC Messages
WAMPAC.3	Improper PDC Configuration Interferes with Relay of Measurement Data
WAMPAC.4	Measurement Data Compromised due to PDC Authentication Compromise
WAMPAC.5	Improper Phasor Gateway Configuration Obscures Cascading Failures
WAMPAC.6	Communications Compromised between PMUs and Control Center
DR.1	Blocked DR Messages Result in Increased Prices or Outages
DR.4	Improper DRAS Configuration Causes Inappropriate DR Messages
DGM.3	Malicious Code Injected into Substation Equipment via Physical Access
DGM.5	Remote Access used to Compromise DMS
DGM.13	Poor Account Management Compromises DMS and Causes Power Loss
Generic.1	Malicious and Non-malicious Insiders Pose Range of Threats
Generic.2	Inadequate Network Segregation Enables Access for Threat Agents
Generic.3	Portable Media Enables Access Despite Network Controls

Source: Table 4. NESCO, *Electric Sector Failure Scenarios and Impact Analyses*. See <http://assets.fiercemarkets.com/public/sites/energy/reports/300200-NESCORFailureScenariosA-9-13Final.pdf>.

Note: See *Electric Sector Failure Scenarios and Impact Analyses* for further descriptions of failure scenarios.

Figure 4. Draft List of Top Potential Failure Scenarios.

Integrating Electric Subsector Failure Assessments into a Risk Assessment Methodology

Using the potential cybersecurity failure scenarios put forward by NESCO, DOE and EPRI issued a voluntary risk assessment process¹²⁵ for utilities to consider in developing and implementing a plan to manage risks from the six failure scenarios developed by NESCO. Utility strategies for framing, assessing, responding to, and monitoring risk on a continual basis are at the center of the process. NESCO's risk assessment approach is based on DOE's ES-C2M2 model, and risk management is focused on DOE's systems security approach¹²⁶ specific to risks from operating IT and IC systems.

AMI.24 Weak Cryptography Exposes AMI Device Communication

Description: An AMI vendor implements weak cryptography that is easy to crack, allowing access to and modification of configuration or data on that interface.

Relevant Vulnerabilities:

- Implementation of weak or unapproved cryptography.

Impact:

- Cost to upgrade or to replace all devices, if upgrade is not feasible. This impact is expected whether or not a threat agent ever uses this vulnerability to launch an attack,
- Loss of customers' private information, and associated costs,
- Mass disconnect of meters potentially causing circuit breaker trips, resulting in temporary outages until power on the grid can be rebalanced.

Potential Mitigations:

- *Require approved cryptographic algorithms,*
- *Define procedure* in change and configuration management policies and procedures to allow future cryptographic changes,
- *Define procedure* to include security, including cryptography, in the purchasing process,
- *Perform security testing* of security controls during system acceptance testing.

Source: NESCO, *Electric Sector Failure Scenarios and Impact Analyses*. See <http://assets.fiercemarkets.com/public/sites/energy/reports/300200-NESCORFailureScenariosA-9-13Final.pdf>.

Figure 5. Example of a NESCO Failure Scenario Path and Its Mitigation.

Potential Mitigation of Cyber Threats

The electric power industry is mostly in a defensive mode regarding cybersecurity threats. One potential area of increasing importance is intrusion detection, since some reports state that cyber attackers may be on an enterprise's system for years before they are detected.¹²⁷

Much of what is emerging from the collaborative efforts of government, industry and academia appears to be focused on changing the way the electric sector views and operates as an enterprise. Protection of the sector from deliberate disruption was not necessarily a high priority for most utilities, especially before Internet connectivity became common. Cyber and physical security are essential if the enterprise is to fulfil its function, and protection of critical infrastructure of the bulk electric system is a mandatory part of utility system operations.

Because many cybersecurity actions are reactive to the last threat discovered, some experts say that mitigation of cyber threats requires a focus on attackers, not the attacks.¹²⁸ Therefore, they suggest that higher-level cybersecurity postures are thus said to require looking beyond whether “something bad” is happening, and shifting to understanding who authored the malicious software and why.¹²⁹ Finding an answer to these issues means understanding the reason for the attack, and then the appropriate resources can be gathered in building an effective defense. The Financial Services Information Sharing and Analysis Center (FS-ISAC) reportedly uses a team of threat analysts who base cyberattack defenses on safeguarding what they think the attackers are after. FS-ISAC operates “a centralized threat repository and an automated network for rapid distribution of threat information from government and industry sources.”¹³⁰ The ES-ISAC performs a similar function to the FS-ISAC for the electricity subsector, but is said not to match FS-ISAC in technical capabilities yet.

The automated, machine-to-machine information exchange that currently exists at FS-ISAC enables a faster, finer-grained identification and analysis of suspected Internet addresses, malicious software code and other threat indicators than the ES-ISAC currently can achieve. That gives FS-ISAC the potential for advanced search and analysis capabilities, including greater insights into identities and methods of various actors. In other words, FS-ISAC has a great capability to “connect the dots” that reveal critical information about an attack and its authors, according to participants in the programs

...Adoption of faster, more automated threat processing technologies by the electric power sector’s vendors may be the best hope of improving cybersecurity defenses among the hundreds of smaller utilities that can’t afford in-house cyberdefense expertise.¹³¹

NCCIC expects to have such “machine-to-machine sharing of online threat data” capabilities available soon.¹³²

Resilience and Recovery

Renewable electricity in distributed generation¹³³ installations and microgrids¹³⁴ have the potential to resist disruptions to the grid, whether from natural occurrences or cyberattacks, by continuing to generate power if the grid is brought down.¹³⁵ Microgrids can be a partial solution to larger scale resilience as they are sized to meet the power needs of a local community or

institution, and they may also be useful in a major cyber event as a staging point for power outage and recovery workers. But they are also another potential point of access to the grid by a cyberattacker.

The Department of Defense looked at how distributed generation can harden its capabilities to maintain its mission and functions in the case of a major cybersecurity event affecting the Grid. A project called the *Smart Power Infrastructure Demonstration for Energy Reliability and Security* (SPIDERS) program was undertaken to help secure military installations if grid power supplies are disrupted.¹³⁶ One of the goals of the SPIDERS project was to transition military bases from reliance on diesel generators for back-up purposes to other on-site renewable electricity technologies and hydrogen fuel cells. Thus, military facilities could function in the event of a major cyber event and serve as centers for recovery efforts.

Using Distributed Computing for Grid Security

In 2013, NIST initiated the *SmartAmerica Challenge*¹³⁷ to address grid vulnerabilities with a focus on using novel approaches. Since the grid relies on control centers to manage power flows in each area of operation, if that control center's operations are disrupted, reductions in service quality or power outages may occur. One SmartAmerica effort is looking at how a distributed computing approach could make the grid more resilient against both physical and cyberattacks.

Because having a single control center for each section of the grid creates a significant vulnerability threat, the NC State and UNC group within the Smart Energy [Cyber-Physical Systems] team is pursuing the idea of creating a distributed computing system that would disseminate monitoring and control functions across multiple virtual machines in a cloud computing network that overlays the grid.¹³⁸

According to a researcher leading the effort, the advantage of using distributed computing methods is "that if one element of the computing system gets compromised, the other virtual machines could step in to protect the system and coordinate their efforts to keep the Grid functioning."¹³⁹

Preparation for recovery from a potential cyberattack requires consideration of the resiliency of the system. Cyber resiliency can be defined as "the coordinated set of enterprise wide activities designed to help organizations respond to and recover from a variety of cyber incidents, while reducing the cost, impact to business operations, and brand damage."¹⁴⁰ But

for electric utilities, the overall goal is system reliability, and the expenditures that may be required to ensure that the grid is functional are just beginning to be understood.

Responsible entities must protect High- and Medium-Impact BES Cyber Assets and BES Cyber Systems under the access restriction provisions of the CIP rules. In some cases, this may require significant investment, such as creating secure enclosures that meet access restriction requirements. Even where capital investment is not required, resources will be needed to implement and validate protective measures as well as to manage and monitor access and, in some cases, configuration.¹⁴¹

Cybersecurity-Related Concerns of Electric Utilities

While mandatory and enforceable reliability standards exist for BES critical infrastructure protection, electric utilities are concerned about the potential for a major cybersecurity event to result in liability concerns that could have financial ramifications.

Liability from a Potential Major Cyber Event

As businesses involved in a commercial enterprise, utilities are aware that they may be vulnerable from a liability standpoint. While adherence to mandatory standards provides a measure for a “standard of care,” it may not be enough to protect companies from legal actions. The American Public Power Association (APPA) summarized the issue as follows:

APPA is concerned that electric utilities may not be sufficiently protected from liability for negligence claims in failing to protect against such attacks even when they have taken every known precaution. Some states are considering legislation that could protect utilities from liability for cyber attacks, but no state or federal statutes currently exist to insulate electric utilities, including public power entities, from legal action in response to a cyber incident....

This and previous Congresses have considered legislation focusing on cybersecurity proposals which have included provisions that would grant liability protections to critical infrastructure owners and operators affected by cyber incident, but no such protections have been enacted into law.¹⁴²

EEI also voiced its concern over liability protection, and additionally considered the potential for unexpected costs for utilities arising from a potential major cyber event.

Costs associated with emergency mitigation are, by definition, unexpected and thus not included in a utility's rate base. To ensure emergency actions do not put undue financial strain on electric utilities, the industry supports mechanisms for recovering costs. In addition, electric utilities support liability protections for actions taken under an emergency order.¹⁴³

Various federal, state and other jurisdictions may allow utility companies to recover costs of cyber and physical security investments. And, in the event of a major cyber or physical security attack, electric utilities also may seek recovery of these costs from their customers in a public utility commission rates filing.

Cybersecurity Insurance

According to DHS, cybersecurity insurance is generally designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. DHS believes "a robust cybersecurity insurance market could help reduce the number of successful cyberattacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection." DHS goes on to state that many companies (including electric utilities) choose not to carry insurance policies, citing the perceived high cost of those policies and confusion about what they cover.¹⁴⁴

In recent years, the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) has brought together a diverse group of private and public sector stakeholders—including insurance carriers, risk managers, IT/cyber experts, critical infrastructure owners, and social scientists—to examine the current state of the cybersecurity insurance market and how to best advance its capacity to incentivize better cyber risk management.... An October 2012 workshop focused on the challenges facing the "first-party" market which covers direct losses to companies arising from cyber-related incidents—including cyber-related critical infrastructure loss.... Based on what it had learned, NPPD hosted an insurance industry working session in April

2014 to assess three areas where it appeared progress could lead to a more robust first-party market: the creation of an anonymized cyber incident data repository; enhanced cyber incident consequence analytics; and enterprise risk management evangelization.¹⁴⁵

Some electric utilities companies view the likelihood of a major cyberattack as a potentially low risk event.¹⁴⁶ However, in the opinion of one insurance industry broker, “[a] major energy catastrophe—on the same scale as ... Exxon Valdez or Deepwater Horizon—could be caused by a cyberattack, and, crucially, that cover for such a loss is generally not currently provided by the energy insurance market.”¹⁴⁷

Most insurance products available to utilities reportedly cover “relatively minor” occurrences such as data losses, or downtime caused by IT issues “but not major events like explosions at multiple facilities triggered remotely by hackers.”¹⁴⁸ The lack of coverage is said to arise from a clause in the insurance agreements of a number of energy sector companies which specifically exclude damage caused by software, viruses or malicious computer code. The lack of coverage will likely continue as long as the exclusionary clause is in effect. However, the clause is reported to remain because cybersecurity “is not well-understood by the insurance industry, making it difficult to design comprehensive products.”¹⁴⁹ Moreover, appraisers from the large insurance provider Lloyds of London are also reported to have found cybersecurity protection measures as “too weak” for a policy to be offered to power companies.¹⁵⁰

ISSUES

The electric utility industry is composed of many different companies of various sizes and various ownership and financial structures.¹⁵¹ Many utilities seem at present to view the potential for a major cybersecurity event as a low probability concern and to want to balance cybersecurity efforts and expenditures with the perceived risks. NERC’s CIP Version 5 seeks to address that thinking by shifting the focus of utilities to provide the necessary levels of security for BES assets with low, medium, or high system impacts. However, many other joint federal and industry cybersecurity activities are cooperative, with voluntary adoption of the measures and metrics developed. The effectiveness of strategies developed and the levels of adoption of recommendations may require congressional evaluation.

Even with mandatory standards, the six failure scenario domains identified by NESCO¹⁵² illustrate the continuing potential vulnerability of the grid to cyber and physical attacks, or a combination of both. While improved cyber intrusion detection measures are a high priority, these are more likely to come from government-industry partnerships than from the utility industry's efforts alone. However, the advice of several initiatives and observers is essentially for electric utilities to embrace cybersecurity as part of their strategic business planning and operations.¹⁵³ Cyber intrusions of the grid are believed to be happening, which may be seen as an indication that that more needs to be done by electric utilities to make the system secure. Whether electric utilities can make the investment financially (and recruit staff) for such a mission is also an issue.

The threats facing the grid are evolving, and with each new intrusion or cyberattack, priorities to protect the system can shift. But that does not mean previous attacks can be considered past issues. SCADA and other control systems infected by worms such as HAVEX are also vulnerable to other actors who may take advantage of such incursions, using or modifying them for their own purposes. This can be a particular concern if, for example, a worm originated from a nation-state. The threat of retaliation would likely be a deterrent from its use by a nation-state, but a terrorist or similar organization would likely be undeterred by such a consequence, and may use the worm for its own purposes. Given the potential for damage to the nation's economy from a major cyberattack on the grid, some might suggest a greater focus on recovery is needed and should become as much a part of a cybersecurity strategy as are efforts to secure the system.

The bulk electric system is subject to mandatory and enforceable critical infrastructure protection rules for cyber and physical security under the FERC's reliability mandate. However, the energy sector is only one of 16 critical infrastructure sectors identified by DHS. Given that the grid relies on several of the others (for example, for water and fuel transportation), the question of whether these other sectors should also have similar, mandatory standards focused on support of the electric power sector may be an issue for Congress to consider.

Additionally, FERC still asserts that it does not have the ability to react to a "fast moving or imminent" cyberattack. Congress may want to consider whether FERC should have more authority to deal with cybersecurity threats in real time.

Congress enacted provisions in EPACT giving the Federal Energy Regulatory Commission responsibility for the reliability of the grid. EPACT

specifically restricted FERC from exercising its reliability authority over distribution systems. Even with the recent redefinition of the BES, there are many points to access the grid beyond those covered by CIP standards from which a potential cyberattack could be launched. Congress may want to consider whether further protection of the grid is necessary, especially along the seams between the newly revised BES and distribution systems beyond FERC's reliability authority. Such actions may include standards (voluntary or mandatory) or defined best practices for facilities connecting to the grid at, for example, a specified voltage level below the bright-line threshold of 120 kV.

Congress may want to consider ways to help companies deal with the costs of critical infrastructure protection. All BES designated facilities (whether these are low, medium or high risk) under CIP Version 5 will be covered by some level of the new requirements. Since the regulatory jurisdictions and financial structures of companies in the electric power industry can differ considerably, Congress may want to look at ways to lessen possible financial strains on electric utility systems with legitimate cost-compliance burden concerns.

Congress may also want to consider liability protection for electric utilities in the event of a major cyberattack. The coverage extended by insurance company products currently available may not extend to damage caused by a cyberattack.

SELECTED PENDING LEGISLATION¹⁵⁴

The following bills are related to cybersecurity issues presented in this report. While not specific to electric utilities, they address information sharing generally between federal and private sector companies. Electric utility companies would argue that the protections and two-way information sharing of the types proposed by these bills would likely promote disclosure of cyber incidents, thus potentially improving cybersecurity for all participants.¹⁵⁵

H.R. 1731 among other actions would amend the Homeland Security Act of 2002 (P.L. 107-296) to enhance multidirectional sharing of information related to cybersecurity risks and strengthen privacy and civil liberties protections. The bill would allow for sharing of cyber threat indicators and other information related to cybersecurity risks and incidents with federal and nonfederal entities, including across sectors of critical infrastructure. The National Cybersecurity and Communications Integration Center (NCCIC) may enter into a voluntary information-sharing relationship with any consenting

nonfederal entity for the purpose of sharing of cyber threat indicators and defensive measures. A nonfederal entity, not including a state, local, or tribal government that shares cyber threat indicators or defensive measures through the NCCIC, shall be deemed to have voluntarily shared such information.

Table 1. Pending Legislation 114th Congress

Bill No.	Title	Committee(s)	Date Introduced	Latest Major Action	Date
H.R. 1731	National Cybersecurity Protection Advancement Act of 2015	Homeland Security	April 13, 2015	Referred to the House Committee on Homeland Security	April 13, 2015
H.R. 234	Cyber Intelligence Sharing and Protection Act	Armed Services, Homeland Security, Intelligence (Permanent), Judiciary	January 8, 2015	Referred to the Subcommittee on the Constitution and Civil Justice.	February 2, 2015
H.R. 85	Terrorism Prevention and Critical Infrastructure Protection Act of 2015	Homeland Security	January 6, 2015	Referred to Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies.	January 23, 2015
S. 456	Cyber Threat Sharing Act of 2015	Homeland Security and Governmental Affairs	February 11, 2015	Referred to the Committee on Homeland Security and Governmental Affairs.	February 11, 2015

Source: Compiled by the Congressional Research Service from Congress.gov.

H.R. 234 among other actions would direct the federal government to provide for the real-time sharing of actionable, situational cyber threat information between all designated federal cyber operations centers to enable integrated actions to protect, prevent, mitigate, respond to, and recover from cyber incidents. The bill also would allow the federal intelligence community

to share cyber threat intelligence with private-sector entities and utilities possessing appropriate certifications or security clearances.

H.R. 85 among other actions would direct DHS to (1) work with critical infrastructure owners and operators and other state and local authorities to take proactive steps to manage risk and strengthen the security and resilience of the nation's critical infrastructure against terrorist attacks; (2) establish terrorism prevention policy to engage with international partners to strengthen the security and resilience of domestic critical infrastructure and critical infrastructure located outside of the United States; (3) establish a task force to conduct research into the best means to address the security and resilience of critical infrastructure in an integrated, holistic manner to reflect critical infrastructure's interconnectedness and interdependency; (4) establish the Strategic Research Imperatives Program to lead DHS's federal civilian agency approach to strengthen critical infrastructure security and resilience; and (5) make available research findings and guidance to federal civilian agencies for the identification, prioritization, assessment, remediation, and security of their internal critical infrastructure to assist in the prevention, mediation, and recovery from terrorism events. The bill also directs DHS to facilitate the timely exchange of terrorism threat and vulnerability information as well as information that allows for the development of a situational awareness capability for federal civilian agencies during terrorist incidents.

S. 456 among other actions would permit private entities to (1) disclose lawfully obtained cyber threat indicators to a private information sharing and analysis organization and the NCCIC; and (2) receive indicators disclosed by private entities, the federal government, or state or local governments. Liability protection would be given to entities that voluntarily share lawfully obtained indicators with NCCIC or a private information sharing and analysis organization if the organization self-certifies that it has adopted the best practices identified by the DHS-selected private entity.

End Notes

¹ Cybersecurity may be defined as the secure (i.e., protected from outside intrusion, corruption or other unauthorized access) operation of networks, computers, hardware, and software systems for business and industrial control processes.

² The Energy Independence and Security Act (EISA) of 2007 (P.L. 110-140) outlined requirements for "a reliable and secure electricity infrastructure" with regard to electric system modernization and Smart Grid development. EISA directed the National Institute of

Standards and Technology (NIST) to develop a framework for protocols and standards for the Smart Grid to achieve “interoperability” of devices and systems.

³ Analog systems can represent cybersecurity vulnerabilities, especially if these are modem-connected and the modem is unsecured. U.S. Department of Homeland Security, National Cyber Security Division, *Recommended Practice for Securing Control System Modems*, January 2008, https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/SecuringModems.pdf.

⁴ See <http://www.dhs.gov/critical-infrastructure-sectors>.

⁵ According to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), there were 140 cyber incidents reported in 2011, 197 in 2012, and 257 cyber incidents reported in 2013. Of the incidents reported in 2013, 56% were directed at energy critical infrastructure, with most directed against electricity infrastructure. This can be compared with 2012, in which 41% of incidents involved energy (again, mostly electricity) facilities. See https://icscert.us-cert.gov/sites/default/files/documents/Year_In_Review_FY2013_Final.pdf.

⁶ The Federal Energy Regulatory Commission (FERC) adopted the North American Electric Reliability Corporation’s (NERC’s) Critical Infrastructure Protection (CIP) Version 5 standards for cybersecurity in April 2014 and subsequently adopted NERC CIP-014 for reliability standards addressing risks due to physical security threats and vulnerabilities in May 2014. See CRS Report R43604, *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*, by Paul W. Parfomak.

⁷ As will be discussed later in this report, a new set of cybersecurity standards have been revised to emphasize security over compliance and go into effect later this year.

⁸ “Other critical infrastructure entities, such as depository institutions in the banking and finance sector; the bulk power system in the electricity subsector of the energy sector; the health care and public health sector; and the nuclear reactors, materials, and waste sector, are required to meet mandatory cybersecurity standards established by federal regulation.” U.S. Government Accountability Office, *Cybersecurity - National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187, February 2013, p. 47, <http://www.gao.gov/assets/660/652170.pdf>.

⁹ The bulk power system includes electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kilovolts or higher. The bulk power system generally does not include distribution system facilities, which are regulated by state or local authorities. See http://www.nerc.com/files/Glossary_2009April20.pdf.

¹⁰ FERC received primary responsibility for the reliability of the bulk power system from the Energy Policy Act of 2005 (P.L. 109-58).

¹¹ The bus bar is the point at which electrical power from the power plant is connected to transmission system.

¹² “The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software.” See Keith Stouffer, Joe Falco, and Karen Scarfone, *Guide to Industrial Control Systems (ICS) Security*, National Institute of Standards and Technology, NIST Special Publication 800-82, June 2011, <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>. (Hereinafter NISTICS).

¹³ Ibid.

¹⁴ Ibid.

- ¹⁵ “RTUs are field devices often equipped with wireless radio interfaces to support remote situations where wire-based communications are unavailable.” NISTICS.
- ¹⁶ Stew Magnuson, “Power Companies Struggle to Maintain Defenses Against Cyberattack,” *National Defense Magazine*, March 2014, <http://www.nationaldefensemagazine.org/archive/2014/March/Pages/PowerCompaniesStruggletoMaintainDefensesAgainstCyberattacks.aspx>.
- ¹⁷ “[These] vulnerabilities ... had been overlooked because taking advantage of them requires an attacker to have access to closed, local networks. Now, a cyberterrorist with a little knowledge and the right laptop can gain that access and cause chaos in a regional power system merely by linking up with the control panel at a secluded electric vehicle charging station.” See Evan Halper, “Security holes in power grid have federal officials scrambling,” *Los Angeles Times*, April 7, 2014, <http://touch.latimes.com/#section/-1/article/p2p-79841438/>. (Hereinafter CyberLT).
- ¹⁸ “A computer worm differs from a virus in that the latter requires user action to set in motion of set of potential harmful activities whereas a worm is self-executable and will burrow its way through an operating system until it reaches its intended target.” For more on Stuxnet, see CRS Report R41524, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, by Paul K. Kerr, John W. Rollins, and Catherine A. Theohary.
- ¹⁹ NISTICS.
- ²⁰ American Society of Civil Engineers, *Report Card for America’s Infrastructure 2013*, p. 2013, <http://www.infrastructurereportcard.org/energy/>.
- ²¹ Department of Energy, *Enhancing the Smart Grid: Integrating Clean Distributed and Renewable Generation*, 2009, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/RDSI_fact_sheet-090209.pdf.
- ²² CRS Report R41886, *The Smart Grid and Cybersecurity—Regulatory Policy and Issues*, by Richard J. Campbell.
- ²³ IEEE Smart Grid, *IEEE Smart Grid Cyber Security Round Up*, 2015.
- ²⁴ CyberLT.
- ²⁵ Louise Downing and James Polson, “Hackers Find Open Back Door to Power Grid With Renewables,” *Bloomberg Business*, July 2, 2014, <http://www.bloomberg.com/news/articles/2014-07-01/renewable-energy-s-expansion-exposinggrids-to-hacking>.
- ²⁶ Christoph Steitz and Harro Ten Wolde, “Smart Meters Pose New Risks for Energy Industry,” *Insurance Journal*, July 18, 2014, <http://www.insurancejournal.com/news/international/2014/07/18/335214.htm>.
- ²⁷ Ibid.
- ²⁸ Ibid.
- ²⁹ Paul Newton, “Security, security, security: the mantra for smart meter data,” *UtilityWeek*, May 26, 2010, <http://www.utilityweek.co.uk/news/Security-security-security-the-mantra-for-smart-meter-data/765952>.
- ³⁰ Energy Sector Control Systems Working Group, *Cybersecurity Procurement Language for Energy Delivery Systems*, April 2014, http://energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguageEnergyDeliverySystems_040714_fin.pdf.
- ³¹ Debra van Opstal, *Supply Chain Solutions for Smart Grid Security: Best Practices*, U.S. Resilience Project, 2012, <https://www.controlsystmsroadmap.net/ieRoadmap%20Documents/SupplyChain-Solutions-for-Smart-GridSecurity.pdf>.
- ³² Ibid.

-
- ³³ Peter Behr, "Cyberattackers have penetrated U.S. infrastructure systems—NSA chief," *Environment & Energy Daily*, November 21, 2014, <http://www.eenews.net/energywire/stories/1060009391>.
- ³⁴ Peter Behr, "As Smart Grid Expands, So Does Vulnerability to Cyber Attacks," *New York Times*, November 19, 2009, <http://www.nytimes.com/cwire/2009/11/19/19climatewire-as-smart-grid-expands-so-does-vulnerability25941.html?pagewanted=all>.
- ³⁵ Malware is a computer program intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system.
- ³⁶ "The most dangerous malware. Trojans are written with the purpose of discovering your financial information, taking over your computer's system resources, and in larger systems creating a 'denial-of-service' (DDOS) attack." A denial-of-service attack is an attempt to make a machine or network resource unavailable to those attempting to reach it. See <http://www.malwaretruth.com/the-list-of-malware-types/>.
- ³⁷ See ICS-CERT alert at <https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B>. (Hereinafter ICSBlack).
- ³⁸ "Spam is unsolicited email, normally with an advertising content sent out as a mass mailing." See <http://www.pandasecurity.com/homeusers/security-info/types-malware/spam/>.
- ³⁹ ICSBlack.
- ⁴⁰ "Advanced Persistent Threats (APTs) are a cybercrime category directed at business and political targets. APTs require a high degree of stealthiness over a prolonged duration of operation in order to be successful. The attack objectives therefore typically extend beyond immediate financial gain, and compromised systems continue to be of service even after key systems have been breached and initial goals reached." See <https://www.damballa.com/advanced-persistent-threats-a-brief-description/>.
- ⁴¹ Stephen Hsieh and Aravind Swaminathan, "BlackEnergy Malware Highlights Special Confidentiality Considerations in Critical Infrastructure Breach Investigations," *JD Supra*, November 18, 2014, <http://www.jdsupra.com/legalnews/blackenergy-malware-highlights-special-c-97560/>. (Hereinafter JDS).
- ⁴² ICSBlack.
- ⁴³ JDS.
- ⁴⁴ CrowdStrike, *Global Threat Report*, 2013, <http://www.crowdstrike.com/new-crowdstrike-report-offersunprecedented-insight-on-worlds-most-sophisticated-cyberattackers-3/>.
- ⁴⁵ "Unlike regular phishing, which sends large numbers of emails to large numbers of people, spear-phishing refers to sending a phishing email to a particular person or relatively small group. Attackers may also heavily customize their spear-phishing emails, using public information gleaned from the Web, to make the emails seem more authentic." See <http://www.darkreading.com/attacks-and-breaches/spear-phishing-attacks-on-the-rise/d-d-id/1098188>.
- ⁴⁶ Daavid Hentunen and Antti Tikkanen, "Havex Hunts For ICS/SCADA Systems," *F-Secure*, June 23, 2014, <https://www.f-secure.com/weblog/archives/00002718.html>.
- ⁴⁷ Ibid.
- ⁴⁸ Heather MacKenzie, "Dragonfly Malware Targets ICS Systems," *Tofino Security*, August 8, 2014, <https://www.tofinosecurity.com/blog/dragonfly-malware-targets-ics-systems>. (Hereinafter Dragonfly).
- ⁴⁹ "It is believed that the Dragonfly group is based in Eastern Europe, and that it is possibly being directed by Russia with state sponsorship involved." Ibid.

- ⁵⁰ Symantec, “*Emerging Threat: Dragonfly/Energetic Bear – APT Group*,” July 30, 2014, <http://fortunascorner.com/2014/07/01/massive-cyberattack-dragonfly-compromised-1k-power-plants-world-wide/>.
- ⁵¹ Dragonfly.
- ⁵² The attack relies on a vulnerability in Windows known as CVE-2014-4114, patched in Bulletin MS14-060.
- ⁵³ “[T]he attack used by Sandworm a so-called zero-day exploit, because the vulnerability was first exploited before a patch was available.” Paul Ducklin, “The ‘Sandworm’ malware - what you need to know,” *Sophos*, October 15, 2014, <https://nakedsecurity.sophos.com/2014/10/15/the-sandworm-malware-what-you-need-to-know/>.
- ⁵⁴ Adam Greenberg, “‘Sandworm Team’ exploits zero-day bug in espionage campaign,” *SCMagazine*, October 14, 2015, <http://www.scmagazine.com/sandworm-team-exploits-zero-day-bug-in-espionage-campaign/article/377238/>.
- ⁵⁵ Kyle Wilhoit and Jim Gogolinski, “Sandworm to Blacken: The SCADA Connection,” *TrendLabs Security Intelligence Blog*, October 17, 2014, <http://blog.trendmicro.com/trendlabs-security-intelligence/sandworm-to-blackenthe-scada-connection/>.
- ⁵⁶ *Ibid.*
- ⁵⁷ FERC Order No. 773 establishes a “bright-line” threshold essentially considering all transmission facilities and related facilities operating at 100 kilovolts or above to be part of the bulk electric power system. As such, these facilities are subject to the applicable NERC reliability standards.
- ⁵⁸ See <http://www.ferc.gov/about/offices/oeis.asp>.
- ⁵⁹ “However, as has been stated by FERC staff and members of the Commission in the past, the tools FERC currently has available to it are inadequate in the face of a fast moving or imminent [cyber]attack, and to the degree FERC does have authority it is limited to the bulk power system and not the myriad of other systems that interact with it. The FERC-NERC standard setting process does have the ability, over time, to create a security ecosystem that makes it much harder for cyber attacks to be successful. But that process is too slow and too open to deal with threats in real time.” Federal Energy Regulatory Commission, *Written Testimony of Commissioner Tony Clark, Federal Energy Regulatory Commission, Before the Committee on Energy and Commerce Subcommittee on Energy and Power United States House of Representatives Hearing on FERC Perspective: Questions Concerning EPA’s Proposed Clean Power Plan and other Grid Reliability Challenges Reliability Challenges*, July 29, 2014, <http://www.ferc.gov/CalendarFiles/20140729091839-Clark-07-29-2014.pdf>.
- ⁶⁰ See “What FERC Does” at <http://www.ferc.gov/about/ferc-does.asp>.
- ⁶¹ “[T]he NERC-CIP framework has important limitations. First, NERC-CIP primarily covers only generation and transmission assets that qualify as ‘critical assets’ or ‘critical cyber-assets.’ With grid modernization, this identification is becoming increasingly problematic as many assets, such as advanced meters, do not fall under NERC-CIP but can have a major impact on grid reliability, safety and customer privacy. Estimates range from 80 percent to over 90 percent of grid assets are outside NERC-CIP’s scope today. Second, NERC-CIP is primarily a compliance-based policy. Compliance is an important component of addressing cybersecurity, but it is not enough to ensure that the rapidly evolving risks are adequately considered and acted upon effectively.” Elizaveta Malashenko, Chris Villarraea, and J. David Erickson, *Cybersecurity and the Evolving Role of State Regulation: How it Impacts the California Public Utilities Commission*, California Public Utilities Commission, Grid Planning and Reliability Policy Paper, September 19, 2012, <http://www.cpuc.ca.gov/NR/rdonlyres/D77BA276-E88A-4C82->

AFD2-FC3D3C76A9FC/0/

TheEvolvingRoleofStateRegulationinCybersecurity9252012FINAL.pdf.

⁶² See FERC Order No. 693, FERC Stats. & Regs. 31,242 at page 77.

⁶³ See 139 FERC 61,247.

⁶⁴ Real (or active) power is the “component of electric power that performs work, typically measured in kilowatts (kW) or megawatts (MW).” See <http://www.eia.gov/tools/glossary/index.cfm>.

⁶⁵ Reactive power is the “portion of electricity that establishes and sustains the electric and magnetic fields of alternating-current equipment. Reactive power must be supplied to most types of magnetic equipment, such as motors and transformers. Reactive power is provided by generators, synchronous condensers, or electrostatic equipment such as capacitors and directly influences electric system voltage. It is a derived value equal to the vector difference between the apparent power and the real power. It is usually expressed as kilovolt-amperes reactive (KVAR) or megavoltampere reactive (MVAR).” See <http://www.eia.gov/tools/glossary/index.cfm>.

⁶⁶ “U.S: New Cybersecurity Organization to Defend Power Grid, March 5,” *Israel Homeland Security*, March 5, 2014, http://i-hls.com/2014/03/u-s-new-cybersecurity-organization-defend-power-grid/?utm_source=rss&utm_medium=rss&utm_campaign=u-s-new-cybersecurity-organization-defend-power-grid.

⁶⁷ NERC CIP Version 5 goes into effect in July 2015. See <http://www.nerc.com/pa/CI/Pages/Transition-Program.aspx>.

⁶⁸ “[A] wide range of assets were excluded simply by avoiding the use of routable communication protocols. The result was that a broad swath of generation facilities had virtually no compliance obligations under the CIP standards.” Steven Parker, “Introduction to NERC CIP Version 5,” *POWER Magazine*, June 1, 2014, <http://www.powermag.com/introduction-to-nerc-cip-version-5/>. (Hereinafter POWERC5).

⁶⁹ Ibid.

⁷⁰ BES replaces “cyber assets” and “critical cyber assets” in NERC CIP terminology.

⁷¹ POWERC5.

⁷² “NERC CIP Version 5: One Giant Leap,” *The State of Security Newsletter*, June 30, 2015, <http://www.tripwire.com/state-of-security/regulatory-compliance/nerc-cip-version-5-one-giant-leap/>.

⁷³ Celia David and Ken Lotterhos, *Transition to NERC CIP Version 5: The Bumpy Road Ahead*, Navigant Consulting, March 2014, http://www.navigant.com/~media/WWW/Site/Insights/Energy/EN_TransitionToNERCCIPVersion5_TL_0314.ashx.

⁷⁴ Siobhan Gorman, “U.S. Plans Cyber Shield for Utilities, Companies,” *Wall Street Journal*, July 8, 2010, <http://www.wsj.com/articles/SB10001424052748704545004575352983850463108>.

⁷⁵ The budget proposes \$149 million for current federal programs focused on improving the cybersecurity of private sector partners of government programs. It includes another \$243 million to support research and development at civilian agencies for innovative cybersecurity technologies. See White House, “Middle Class Economics: Cybersecurity,” *The President’s Budget FY2016*, 2015, https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/cybersecurity.pdf.

⁷⁶ DOE, Office of Electricity Delivery and Energy Reliability, *Cybersecurity*, 2015, <http://energy.gov/oe/services/cybersecurity>.

⁷⁷ P.L. 111-85. See Title III, DOE Energy Programs.

⁷⁸ See <http://energy.gov/oe/services/cybersecurity/nesco>.

⁷⁹ See <http://www.energysec.org/services/advisory-services/>.

⁸⁰ See <http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program>.

⁸¹ See “Electricity Subsector Cybersecurity Capability Maturity Model Version 1.1” at <http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf>.

⁸² The update discussed roadmaps for improving areas such as intrusion detection and development of metrics for measuring security improvements. See U.S. Department of Energy, Energy Sector Control Systems Working Group, *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, September 2011, http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf.

⁸³ DHS was established by the Homeland Security Act of 2002 (P.L. 107-296).

⁸⁴ DHS, “About the National Protection and Programs Directorate - Divisions,” <http://www.dhs.gov/about-nationalprotection-and-programs-directorate>.

⁸⁵ DHS, “About the National Cybersecurity and Communications Integration Center,” November 4, 2014, <http://www.dhs.gov/about-national-cybersecurity-communications-integration-center>. (Hereinafter NCCIC).

⁸⁶ Ibid.

⁸⁷ Ibid.

⁸⁸ See <https://www.us-cert.gov/>.

⁸⁹ See <https://ics-cert.us-cert.gov/>.

⁹⁰ See DHS, *National Cybersecurity Protection System*, Detection, April 2, 2014, <http://www.dhs.gov/nationalcybersecurity-protection-system-ncps>.

⁹¹ See CRS Report R43941, *Cybersecurity and Information Sharing: Legal Challenges and Solutions*, by Andrew Nolan.

⁹² See <http://www.dhs.gov/science-and-technology>.

⁹³ See <http://www.dhs.gov/science-and-technology/cyber-security-division>.

⁹⁴ DHS considers the development and testing of the recovery transformer to be a success. See U.S. Congress, House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, *The DHS and DOE National Labs: Finding Efficiencies and Optimizing Outputs in Homeland Security Research and Development*, 112th Cong., 2nd sess., April 19, 2012, H. Hrg. 112-84 (Washington: GPO, 2013), pp. 7-11. DOE is now looking at the need to develop a stockpile of transformers for use in an EMP event (See <http://www.eenews.net/energywire/stories/1060014919>).

⁹⁵ See <http://www.dhs.gov/science-and-technology/about-st>.

⁹⁶ National Institute of Standards and Technology, Smart Grid Interoperability Panel Cyber Security Working Group, Introduction to NISTIR 7628, *Guidelines for Smart Grid Cyber Security*, September 2010, <http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf>. (Hereinafter NISTIR).

⁹⁷ NISTIR, p. 9.

⁹⁸ NIST first published the report in 2010. The current version was released in September 2014 as NISTIR 7628 Revision 1. See http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf.

⁹⁹ NIST, *Cybersecurity for Smart Grid Systems*, January 24, 2014, <http://www.nist.gov/el/smartgrid/cybersg.cfm>.

¹⁰⁰ Interoperability can be defined as the capability of two or more networks, systems, devices, applications, or components to share and readily use information securely and effectively with little or no inconvenience to the user. GridWise Architecture Council, Interoperability

- Path Forward Whitepaper, November 30, 2005, http://www.gridwiseac.org/pdfs/interoperability_path_whitepaper_v1_0.pdf.
- ¹⁰¹ See <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructurecybersecurity>.
- ¹⁰² CRS Report R42984, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, by Eric A. Fischer et al.
- ¹⁰³ NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014, <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.
- ¹⁰⁴ See <https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructurecybersecurity>.
- ¹⁰⁵ See <http://nccoe.nist.gov/>.
- ¹⁰⁶ See <http://www.nerc.com/comm/CIPC/Pages/default.aspx>.
- ¹⁰⁷ See NERC, *ES-ISAC*, 2013, <http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>.
- ¹⁰⁸ See <https://www.esisac.com/SitePages/FAQ.aspx>.
- ¹⁰⁹ NERC members must apply to ES-ISAC to become registered entities. “The ES-ISAC is reviewing its policy regarding integrating potential external parties and their expertise and capabilities with the ES-ISAC.” See <https://www.esisac.com/SitePages/FAQ.aspx>.
- ¹¹⁰ “All registered entities in the North American electricity sector may be participants in the ES-ISAC. Although the ISAC framework is a U.S. government construct, the ES-ISAC extends across all of NERC’s territory, which includes both Canada and portions of Mexico.... Registered entities who are members of the ES-ISAC received private-level information on security threats, including alerts; remediation; various task forces; events calendars; and other security-specific resources.” See <https://www.esisac.com/SitePages/FAQ.aspx>.
- ¹¹¹ The Energy Critical Infrastructure sector includes the electricity, petroleum, and natural gas subsectors. See <http://www.dhs.gov/critical-infrastructure-sectors>.
- ¹¹² See <http://www.dhs.gov/national-infrastructure-protection-plan>.
- ¹¹³ Edison Electric Institute, *Electric Subsector Coordinating Council*, March 2015, <http://www.eei.org/issuesandpolicy/cybersecurity/Documents/ESCC%20Brochure.pdf>.
- ¹¹⁴ Ibid.
- ¹¹⁵ Edison Electric Institute, *Electric Power Industry Initiatives To Protect The Nation’s Grid From Cyber Threats*, October 2014, <http://www.eei.org/issuesandpolicy/cybersecurity/Documents/EEI%20Cybersecurity%20Backgrounder.pdf>.
- ¹¹⁶ National Electric Sector Cybersecurity Organization, Technical Working Group 1, *Electric Sector Failure Scenarios and Impact Analyses*, September 2013, <http://assets.fiercemarkets.com/public/sites/energy/reports/300200NESCORFailureScenario sA-9-13Final.pdf>. (Hereinafter NESCFail).
- ¹¹⁷ NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, Special Publication 1108, January, 2010, http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.
- ¹¹⁸ Advanced Metering Infrastructure (AMI) is intended to “implement residential demand response and to serve as the chief mechanism for implementing dynamic pricing. It consists of the communications hardware and software and associated system and data management software that creates a two-way network between advanced meters and utility business systems, enabling collection and distribution of information to customers and other parties, such as the competitive retail supplier or the utility itself. AMI provides customers real-time (or near real-time) pricing of electricity, and it can help utilities achieve necessary load reductions.” NESCFail.

- ¹¹⁹ “DER systems are “cyber-physical systems that provide energy and ancillary services to the power grid, typically through the distribution system. DER systems can be generators, storage devices, and even electric vehicles if their chargers are capable of managing the charging and discharging processes. Generally DER systems are small,” but they are becoming prevalent in the distribution system (potentially there will be thousands if not millions of DER systems interconnected with the distribution system).” Ibid.
- ¹²⁰ “Wide Area Monitoring, Protection, and Control (WAMPAC) ... systems constitute a suite of different system solutions aimed at meeting various wide-area application requirements. WAMPAC systems often center around synchrophasor technology and the devices that generate, receive, and utilize this synchrophasor data. WAMPAC systems should be setup to include all components from the Phasor Measurement Unit (PMU) to the WAMPAC applications leveraging that data, including other intermediate devices such as the servers that manage the PMUs, devices that provide alignment services like Phasor Data Concentrators (PDCs), phasor gateways, phasor data stores, and other such components.” Ibid.
- ¹²¹ “Electric Transportation (ET) ... systems are setup to include components starting ‘from the Electric Vehicle (EV) and the Electric Vehicle Supply Equipment (EVSE) to the EV Management Server hat communicates with the EVSEs. The EV may have an in-vehicle system that is connected to the battery through the vehicle’s Car Area Network (CAN) that exchanges data with the EVSE via a wireless channel or PLC.... ET systems also include other intermediate devices. A meter measures power usage for each EVSE. A gateway collects data from the meters and the EVSEs and transmits the data to the EV Management Server.” Ibid.
- ¹²² “Demand Response (DR) communications cover interactions between wholesale markets and retail utilities and aggregators, as well as between these entities and the end-load customers who reduce demand in response to grid reliability or price signals. [...] Price (often with the time that the price is effective), grid integrity signals (e.g., event levels of low, medium, high), and possibly environmental signals (e.g., air quality) are components of DR communications.” Ibid.
- ¹²³ Distribution Grid Management (DGM) “focuses on maximizing performance of feeders, transformers, and other components of networked distribution systems and integrating with transmission systems and customer operations. As Smart Grid capabilities, such as AMI and demand response, are developed, and as large numbers of distributed energy resources and plug-in electric vehicles (PEVs) are deployed, the automation of distribution systems becomes increasingly more important to the efficient and reliable operation of the overall power system.” Ibid.
- ¹²⁴ NESCFAIL.
- ¹²⁵ DOE, EPRI, *Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology*, 3002001181, December 2013, <http://energy.gov/sites/prod/files/2014/04/f14/IntegratingElectricitySubsectorFailureScenariosIntoARiskAssessmentMethodology.pdf>.
- ¹²⁶ DOE, *Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline*, May 2012, <http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf>.
- ¹²⁷ Paz Eshel, Bucky Moore, and Shiran Shalev, *Why Breach Detection Is Your New Must-Have, Cyber Security Tool*, TechCrunch, September 6, 2014, <http://techcrunch.com/2014/09/06/why-breach-detection-ss-your-new-must-havecyber-security-tool/>.

- ¹²⁸ Peter Behr, “In fighting cyber crimes, experts call for focus on attackers, not attacks,” *EnergyWire*, June 17, 2014, <http://www.eenews.net/energywire/2014/06/17/stories/1060001405>. (Hereinafter FOACS).
- ¹²⁹ Ibid.
- ¹³⁰ Ibid.
- ¹³¹ Ibid.
- ¹³² NPPD Under Secretary Suzanne Spaulding and NPPD Deputy Under Secretary for Cybersecurity & Communications Phyllis Schneck, *Hearing on Examining the President’s Cybersecurity Information Sharing Proposal*, House Committee on Homeland Security, Building Capacity to Accelerate Automated Sharing of Cyber Threat Indicators, February 25, 2015, <http://www.dhs.gov/news/2015/02/25/written-testimony-nppd-under-secretary-anddeputy-under-secretary-cybersecurity>.
- ¹³³ DOE defines distributed generation as “electric generation that feeds into the distribution grid, rather than the bulk transmission grid, whether on the utility side of the meter, or on the customer side.” Distributed generation encompasses a wide range of technologies including solar photovoltaic (PV) panels, combined heat and power systems, backup generators powered by a variety of fuels, small wind turbines, fuel cells, microturbines, and energy storage devices. DOE, *The Potential Benefits of Distributed Generation and Rate-Related Issues that May Impede Their Expansion*, February 2007, http://www.ferc.gov/legal/fed-sta/exp-study.pdf#xml=http://search.atomz.com/search/pdfhelper.tk?sp_o=12,100000,0.
- ¹³⁴ “A microgrid is a localized grouping of electricity sources and loads that normally operates connected to and synchronous with the traditional centralized grid (macrogrid), but can disconnect and function autonomously as physical and/or economic conditions dictate.” DOE, Berkeley Laboratory, “About Microgrids,” 2015, <https://building-microgrid.lbl.gov/about-microgrids>.
- ¹³⁵ Smart inverters allow these systems to continue providing generated power to the connected host even if the grid is not operational.
- ¹³⁶ SPIDERS was led by Sandia National Laboratories, under a partnership between the Department of Defense and the Department of Energy that involves numerous other federal laboratories, agencies and military commands. Tina Casey, *In First Test, U.S. Military’s SPIDERS Microgrid Uses 90% Renewable Energy*, CleanTechnica, February 12, 2013, <http://cleantechnica.com/2013/02/12/u-s-militarys-new-spiders-renewable-energy-microgrid/>.
- ¹³⁷ “The SmartAmerica Challenge brings together organizations with Cyber-Physical Systems (CPS) technology, programs, and test beds to demonstrate the potential to improve safety, sustainability, efficiency, mobility, and overall quality of life. Cyber-Physical Systems—sometimes referred to as the Internet of Things (IoT)—involves connecting devices and systems in diverse sectors like transportation, energy, manufacturing, and healthcare in fundamentally new ways.” See <http://www.nist.gov/el/smartamerica.cfm>.
- ¹³⁸ Matt Shipman, “Researchers test distributed computing as defense against cyberattacks on power grids,” PhysicsOrg, May 21, 2014, <http://phys.org/news/2014-05-defense-cyberattacks-power-grids.html>.
- ¹³⁹ Aranya Chakraborty, an assistant professor of electrical engineering who is leading the project from NC State. Ibid.
- ¹⁴⁰ Deloitte Consulting, “From Cyber Incident Response to Cyber Resilience,” *Wall Street Journal*, February 24, 2015. “Cyber resilience—the coordinated set of enterprise-wide activities designed to help organizations respond to and recover from a variety of cyber incidents, while reducing the cost, impact to business operations, and brand damage...”

-
- ¹⁴¹ Celia David and Ken Lotterhos, *Transition to NERC CIP Version 5: The Bumpy Road Ahead*, Navigant Consulting, March 2014, http://www.navigant.com/~media/WWW/Site/Insights/Energy/EN_TransitionToNERCCIPVersion5_TL_0314.ashx.
- ¹⁴² American Public Power Association, *In Support of Appropriate Liability Protection for Electric Utilities Related to Cyber Attacks*, Resolution 14-08, June 17, 2014, <http://publicpower.org/files/PDFs/Resolution%2014-08%20—%20Liability%20Protection%20for%20Utilities%20Related%20to%20Cyber%20Attacks%20—%20FINAL.pdf>.
- ¹⁴³ Edison Electric Institute, *EI Principles for Cybersecurity and Critical Infrastructure Protection*, September 9, 2010, <http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity%20Principles.pdf>.
- ¹⁴⁴ DHS, *Cybersecurity Insurance*, 2015, <http://www.dhs.gov/publication/cybersecurity-insurance>.
- ¹⁴⁵ *Ibid.*
- ¹⁴⁶ See Ron Brown, “Utilities can Prepare for Disasters More Efficiently,” *Electric Light & Power*, July 17, 2013, http://www.elp.com/articles/powergrid_international/print/volume-18/issue-7/features/utilities-can-prepare-fordisasters-more-efficiently.html.
- ¹⁴⁷ “Energy Firms Unprotected for Major Cyber Events: Willis,” *Insurance Journal*, April 15, 2014, <http://www.insurancejournal.com/news/national/2014/04/15/325848.htm>.
- ¹⁴⁸ *Ibid.*
- ¹⁴⁹ *Ibid.*
- ¹⁵⁰ Mark Ward, “Energy firm cyber-defence is ‘too weak’, insurers say,” BBC, February 27, 2014, <http://www.bbc.com/news/technology-26358042>.
- ¹⁵¹ As of 2007, there were 210 investor-owned electric utilities, 2,009 publicly owned electric utilities, 883 consumer-owned rural electric cooperatives, and 9 federal electric utilities. Energy Information Administration (EIA), “Electric Power Industry Overview,” 2007, <http://www.eia.doe.gov/electricity/page/prim2/toc2.html>.
- ¹⁵² See “NESCO Cybersecurity Failure Scenarios,” above.
- ¹⁵³ For example, NERC CIP Version.5 requires BES owners to focus on improving security, not just compliance with standards, and the FS-ISAC focuses on what it perceives as “most valuable to attackers in order to understand where to build defenses.” FOACS.
- ¹⁵⁴ For further information on recently introduced bills addressing cybersecurity issues, see CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by Rita Tehan.
- ¹⁵⁵ For additional discussion of current and proposed cybersecurity legislation, see CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, by Eric A. Fischer.

Chapter 4

PHYSICAL SECURITY OF THE U.S. POWER GRID: HIGH-VOLTAGE TRANSFORMER SUBSTATIONS*

Paul W. Parfomak

SUMMARY

The U.S. electric power grid consists of over 200,000 miles of high-voltage transmission lines and hundreds of large transformer substations. High voltage (HV) transformer units make up less than 3% of U.S. transformers, but they carry 60%-70% of the nation's electricity. Because they serve as vital nodes, HV transformers are critical to the nation's electric grid. HV transformers are also the most vulnerable to damage from malicious acts.

For more than 10 years, the electric utility industry and government agencies have engaged in activities to secure HV transformers from physical attack and to improve recovery in the event of a successful attack. These activities include coordination and information sharing, spare equipment programs, security standards, security exercises, and other measures. There has been some level of physical security investment and an increasing refinement of voluntary security practices across the electric power sector for at least the last 15 years. However, recent grid security exercises, together with a 2013 physical attack on

* This is an edited, reformatted and augmented version of a Congressional Research Service, Publication No. R43604, dated July 2, 2015.

transformers in Metcalf, CA, have changed the way grid security is viewed and have focused congressional interest on the physical security of HV transformers. They have also prompted new grid security efforts by utilities and regulators.

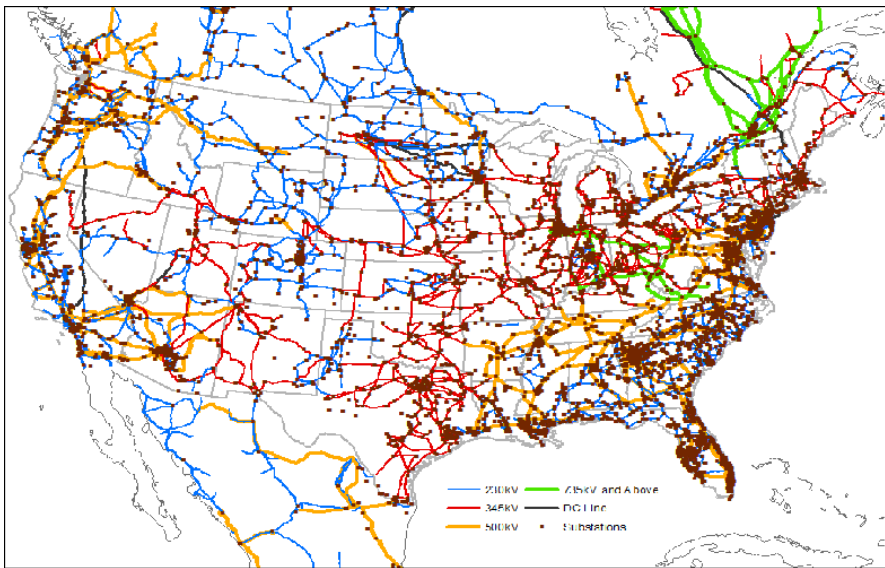
On November 20, 2014, the Federal Energy Regulatory Commission (FERC) approved a new mandatory Physical Security Reliability Standard (CIP-014-1) proposed by the North American Electric Reliability Corporation (NERC). The new standards require certain transmission owners “to address physical security risks and vulnerabilities related to the reliable operation” of the power grid by performing risk assessments to identify their critical facilities, evaluate potential threats and vulnerabilities, and implement security plans to protect against attacks. Legislative proposals would expand federal efforts to prevent or recover from a physical attack on the U.S. grid. These include the Enhanced Grid Security Act of 2015 (S. 1241), the Critical Electric Infrastructure Protection Act (H.R. 2271), the Terrorism Prevention and Critical Infrastructure Protection Act of 2015 (H.R. 85), a House bill to establish a strategic transformer reserve program (H.R. 2244), and the Grid Modernization Act of 2015 (S. 1243).

There is widespread agreement among government agencies, utilities, and manufacturers that HV transformers in the United States are vulnerable to terrorist attack, and that such an attack potentially could have catastrophic consequences. But the most serious, multi-transformer attacks could require acquiring operational information and a certain level of sophistication on the part of potential attackers. Consequently, despite the technical arguments, without more specific information about potential targets and attacker capabilities, the actual risk of a multi-HV transformer attack remains an open question. As the electric power industry and federal agencies continue their efforts to improve the physical security of critical HV transformer substations, Congress may consider several issues as part of its oversight of the sector: identifying critical transformers, confidentiality of critical transformer information, adequacy of HV transformer protection, quality of federal threat information, recovery from HV transformer attacks, and the overall resiliency of the grid. Maintaining an integrated perspective on prevention, recovery, and resilience may help to promote an effective balance among industry investment, regulatory requirements, and federal oversight.

INTRODUCTION¹

The electric utility industry operates as an integrated system of generation, transmission, and distribution facilities to deliver electric power to consumers.

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



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

Figure 1. Electric Transmission Network.

The U.S. electric power grid has historically operated with such high reliability that any major disruption caused by weather, operational errors, or sabotage, makes news headlines. The various parts of the electric power system are all vulnerable to failure due to natural, operational, or manmade events. Such outages can have considerable negative impacts on business, government services, and daily life. Notwithstanding its high reliability overall, the U.S. power grid has periodically experienced major regional outages. Recent examples include the Northeast Blackout of 2003 (which affected 55 million customers in eight states and Canada) and extended

outages in the New York/New Jersey area after Superstorm Sandy in 2012. For reasons discussed below, however, HV transformers are considered by many experts to be the most vulnerable to intentional damage from malicious acts. The physical security of HV transformers and associated policy issues are the subject of this report.

Congressional Interest

Congress has long been concerned about grid security in general, but recent security exercises, together with a 2013 physical attack on transformers in Metcalf, CA, have focused congressional interest on the physical security of HV transformers, among other specific aspects of the grid.⁵ They have also prompted new grid security initiatives by utilities and federal regulators. Legislative proposals including the Enhanced Grid Security Act of 2015 (S. 1241), the Critical Electric Infrastructure Protection Act (H.R. 2271), the Terrorism Prevention and Critical Infrastructure Protection Act of 2015 (H.R. 85), a House bill to establish a strategic transformer reserve program (H.R. 2244), and the Grid Modernization Act of 2015 (S. 1243) would expand these activities by strengthening federal efforts to prevent or recover from a physical attack on the U.S. grid.

HV TRANSFORMER RISKS AND VULNERABILITY

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

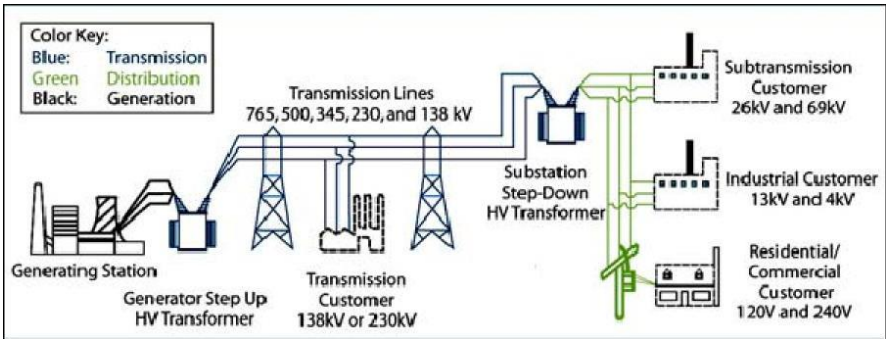
consequences. This section discusses in more detail HV transformer characteristics and physical security risks associated with them.

High Voltage Power Transformers

Utility transformers control the voltage of electricity so that it can be synchronized with other power supplies, transmitted long distances, and distributed to customers. Transformers range in size from small, pole-mounted units that may serve a dozen homes to transmission units that serve an entire city. The larger the transformer, the higher the voltage the transformer can handle. Utility transformers, regardless of size, fundamentally consist of copper wire wrapped around a metallic “core” within an insulated protective housing covered with a 5/8 to 3/4-inch mild steel tank. They are linked to the power grid by protruding metal and (usually) ceramic connectors called “bushings” which resemble giant spark plugs. Larger transformers generate waste heat during operation (like all transformers), so they are cooled by a system comprised of internally circulating oil and external radiators, analogous to the cooling system in a car engine. Large transformers are located in network substations along with transmission lines, associated electric equipment, and system controls. These substations may be found in remote locations or near urban centers, depending upon regional transmission needs. Many are located alongside electric generation plants, linking those plants to the grid.

Voltage Management in the U.S. Power System

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



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

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



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

Figure 3. Installation of a 345 kV Transformer.

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

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

Manufacture and Cost

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

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

U.S. Manufacturing Capability

From 1950 to 1970, utility construction of large generation plants and associated transmission networks fueled a robust U.S. manufacturing market for large transformers. During this period, the United States (and Canada) accounted for approximately 40% of global demand for such units.¹³ After 1970, however, utility investment in transmission infrastructure began falling off due to perceived overcapacity, public resistance to transmission siting, and greater regulatory scrutiny of capital expenditures. Beginning in the late 1980s, uncertainty about industry restructuring and the introduction of competition made grid owners even less willing to invest in new transmission. This decline in U.S. transmission investment greatly reduced domestic demand for large transformers, especially HV transformers. By the late 1990s, the United States and Canada accounted for only 20% of global large transformer

sales.¹⁴ Demand in the United States has subsequently increased, however. For example, between 2005 and 2013, the total value of large transformers (including medium- and high-voltage units) imported to the United States more than doubled, from \$284 million (363 units) to \$676 million (496 units).¹⁵

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

HV Transformer Sites in the United States

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

Criticality of HV Transformers

Because HV transformers carry so much electricity, the destruction of even a small number could seriously reduce the transmission capacity of a regional electric power grid and lead to extended blackouts. The impact of such a failure would depend on the electricity flows in that part of the grid, congestion from major network bottlenecks, and the status of other key

facilities such as power plants, transmission lines, and other substations. Power grid planners generally anticipate the possible loss of a single HV transformer substation and are prepared to reroute power flows as necessary to maintain regional electric service. But the simultaneous loss of multiple HV transformers, especially in a constrained transmission area, could exceed the capability of a regional network to reroute power through secondary lines.¹⁹

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

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

In such an emergency scenario, limited electric service could likely be restored in the short term by imposing “rolling” blackouts, rerouting transmission, and using portable transformers. Nonetheless, the loss of key HV substations would leave the regional network crippled and highly susceptible to further disturbance and cascading failure.²¹ According to power industry experts, certain parts of the U.S. transmission network are particularly vulnerable to HV substation disruption. These areas may have severely constrained transmission paths relying on a small number of HV transformers in extremely critical network locations. According to press accounts, a FERC power flow analysis in 2013 identified 30 such critical HV transformer substations across the continental United States; disabling as few as nine of these substations during a time of peak electricity demand reportedly could cause a “coast-to-coast blackout.”²²

Notwithstanding the FERC study and similar claims by security analysts, the actual risk to the U.S. grid of extended blackouts due to a deliberate attack on multiple HV transformers is the subject of ongoing debate. An investigation by the Department of Energy’s Office of Inspector General (IG) appears to discredit FERC’s risk analysis. According to the IG investigation, officials at the department previously concluded that FERC’s study was based on “highly unlikely assumptions” and that “loss of the critical substations identified in the analysis would not result in the consequence described in the analysis or any

other consequence that could be reasonably expected to result in damage to national security.”²³ Due to the complexity of HV transmission networks and uncertainties about potential physical threats, a range of differing conclusions may be reached by industry experts on the potential severity and duration of a blackout from a multi-transformer attack. However, most analysts acknowledge that severe regional, if not national, power outages may be technically possible under certain conditions.²⁴

Physical Vulnerability of HV Transformers

The Department of Energy’s recent *Quadrennial Energy Review* identifies HV transformers as one of the electric grid’s “most vulnerable components.”²⁵ All HV transformers are designed to withstand operational risks such as lightning strikes, hurricanes, and network power fluctuations—but they are vulnerable to intentional physical attacks. Despite their great size and internal complexity, HV transformers of conventional design can be readily disabled or destroyed. According to one manufacturer, “if someone were to intentionally try ... it is a surprisingly simple task and there are a large number of ways to conceivably damage a transformer beyond repair.”²⁶ Transformer experts have asserted that a bad actor with basic knowledge of transformer design could inflict irreparable damage. Such attacks can cause massive electrical short circuits and oil fires that would destroy an HV transformer and damage surrounding infrastructure. One fire at a 345 kV substation in Texas, for example, destroyed the transformer and burned for five hours, causing “plumes of smoke that could be seen for miles.”²⁷ In addition to direct attacks on the transformers themselves, HV substations can be further disabled by damaging associated transmission lines or control centers that may be located on site.

Because HV transformers are so big and are connected to the largest overhead transmission towers, they are easily identified along major transmission corridors. High voltage transformers are usually housed in substations that are enclosed with a chain-link fence. Guards are not often stationed at these facilities under normal operating circumstances. Consequently, HV transformers are ordinarily easier to access than other critical electric facilities such as generation plants and control centers. Utilities use closed-circuit surveillance and other methods to detect intrusion. However, access to the substation may be achieved by either cutting or scaling the chain-link fence. Once inside, a saboteur could cause damage by accessing the

control room or physically damaging the HV transformer. Penetrating the 5/8 to 3/4-inch steel tank with any device could short-circuit the windings and irreparably destroy the transformer. Alternatively, a saboteur could attempt to open a valve and drain the insulating oil. Igniting the oil might cause the transformer to arc and eventually explode. With a clear line of sight, an attacker could also disable transformers from a distance using conventional rifles. Other methods of disabling HV transformers have also been identified.

The vulnerability of individual transformer substations has been demonstrated by successful attacks in recent years. In the most serious case, a rifle attack occurred in April 2013 at PG&E's 500 kV substation in Metcalf, CA. In this attack, multiple individuals outside the substation reportedly shot at the HV transformer radiators with .30 caliber rounds, causing them to leak cooling oil, overheat, and become inoperative.²⁸ In October 2013, the U.S. Justice Department charged an individual with attacks on the transmission grid in Arkansas, including a deliberate fire at Entergy's 500 kV substation in Lonoke County. The fire consumed the substation control house but electrical service was not interrupted.²⁹ In 2005, at a Progress Energy substation in Florida, a rifle attack ruptured a transformer oil tank, ultimately causing an explosion and local blackout.³⁰ Other incidents at substations have been reported with some regularity, although most have been attributed to vandals or careless hunters.

It is very difficult to restore a damaged HV transformer substation. As noted above, transmission experts assert that most HV transformers currently in service are custom designed and, therefore, cannot be generally interchanged. Furthermore, at \$3-5 million per unit or more, maintaining large inventories of spare HV transformers solely as emergency replacements is prohibitively costly, so limited extras are on hand. The number of spares a utility maintains is increasingly sensitive information, but one regional transmission control area reported in 2007 that it maintained 29 spares for 188 transformers rated 500 kV on its system.³¹ Programs for the sharing of spare HV transformers among multiple utilities are discussed later in this report.

Within the United States, transportation of HV transformers is difficult. Due to their size and weight, most HV transformers are transported on special railcars, each with up to 36 axles to distribute the load. There are fewer than 20 of these railcars in the United States rated to carry 500 tons or more, which can present a logistical problem if they are needed in a transformer emergency.³² In some cases involving older transformers, adjacent rail lines are no longer in service, so replacement transformers may need to be transported by other means. Specialized flatbed trucks can also carry heavy

transformer loads over public roadways, but the few such trucks that exist have less carrying capacity and greater route restrictions than the railcars because HV transformers may exceed highway weight limits. Transporting HV transformers, especially in an emergency, can create other logistical challenges as well, including the coordination of movement through ports and road constraints (e.g., tunnels and overpasses), special transportation permits, and police escort requirements.³³

Targeting of HV Transformers

Malicious individuals could, without significant training, identify critical HV transformer locations and time an attack for greatest effect. This could be accomplished with basic knowledge of transmission operations and regional network characteristics drawn from publicly available sources, including electric marketing data indicating constrained areas of the network.³⁴ In 2014, a security services company published a summary of this kind of exercise, identifying 14 of the “most critical” transformer substations in the United States based on the company’s criteria.³⁵ As stated in a 2012 National Research Council report, “terrorists could selectively target key equipment, especially large transformers.”³⁶ The OTA report describes such a scenario:

[One] example is a city served by eight transmission substations spread along a 250-mile line and located in five States. A knowledgeable saboteur would be needed to identify and find the eight transmission substations. A highly organized attack would also be required. However the damage would be enormous, blacking out a four-State region, with severe degradation of both reliability and economy for months.³⁷

In 1997, the Irish Republican Army reportedly planned this kind of coordinated attack against six transmission substations in the United Kingdom. Although the attack was prevented, had it been successful it reportedly could have caused widespread power outages in London and the South East of England for months.³⁸

It is relatively easy to learn about HV transformer vulnerabilities from engineers and operators experienced with this technology, either domestically or abroad, since the same technology is used in power grids throughout the world. In the past, transformer experts have provided CRS with detailed descriptions of numerous “simple” ways terrorists could destroy HV

transformers. General transformer sabotage information is also available on the Internet. One sabotage manual associated with white supremacist groups available online includes the following discussion:

The power generation and distribution systems of most major Western cities are surprisingly vulnerable.... Attacking during peak consumption times (Winter in cold climates and Summer in hot climates) will make power diversion impossible.... Arson, explosives or long-range rifle fire can be used to disable substations, transformers and suspension pylons. A simultaneous attack against a number of these targets can shut down power ... with the advantage that service cannot be quickly restored by diverting power from another source. Each broken link in the power grid must be repaired in order to fully restore service. An individual, equipped with a silenced rifle or pistol, could easily destroy dozens of power transformers in a very short period of time.³⁹

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

Physical Security Measures for HV Transformers

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

- **Protecting information** about critical HV substations, such as engineering drawings, power flow modeling runs, and site security information, which could be useful to a potential attacker.
- **Surveillance and monitoring** through the use of video cameras, motion detectors, imaging, acoustical monitors, aerial drones, and periodic inspection by security employees.

- **Restricting physical access**, such as limiting entry only to necessary employees, installing electronic locks and other access controls, and erecting physical barriers and controls for vehicle entry. Posting full-time guards may also be an option in some circumstances.
- **Shielding assets** from offsite attacks using visual barriers such as opaque or hardened fencing, erecting taller fences, or erecting protective walls.
- **Modifying substation designs** to make them more resistant to physical damage, for example, by strengthening transformer cooling systems or bushings.
Reconfiguring substation layouts to limit asset visibility or limit the spread of fire may also be options.

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

SECTOR INITIATIVES FOR HV TRANSFORMER SECURITY

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

Coordination and Information Sharing

The *National Infrastructure Protection Plan* (NIPP), initially published by the Department of Homeland Security in 2006, “outlines how government and private sector participants in the critical infrastructure community work

together to manage risks and achieve security and resilience outcomes.”⁴⁰ The plan organizes critical infrastructure into distinct sectors, designating a federal department or agency as the lead coordinator for each sector—the Sector Specific Agency (SSA). Under the NIPP and Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience, the Department of Energy (DOE) is designated as the SSA for the Energy Sector, which includes the electric utility industry (excluding nuclear power plants). As an SSA, the department is responsible for working with the Department of Homeland Security (DHS), other federal agencies, critical infrastructure owners, independent regulators, and other agencies to implement national policy on critical infrastructure security and resilience.⁴¹ The NIPP also established a sector partnership model including private and government coordinating councils:

- The **Electricity Subsector Coordinating Council (ESCC)**, initially established in 2004, was organized and administered by companies in the electric power industry. It meets regularly to coordinate policy-related activities designed to “improve the reliability and resilience of the electricity subsector, including physical and cyber infrastructure.”⁴² Through August 15, 2013, the ESCC was chaired by the North American Electric Reliability Corporation (NERC), the not-for-profit organization responsible for ensuring the reliability of the North American grid.⁴³ The ESCC has since transitioned to a new structure led by electric utility industry executives, although NERC’s chief executive officer remains on the ESCC steering committee.⁴⁴
- The **Energy Sector Government Coordinating Council (EGCC)**, also established in 2004, is the government counterpart to the ESCC. The EGCC is chaired by the DOE and DHS, incorporating other agencies at all levels of government with interest in energy security. The EGCC plays a key role in implementing the Sector-Specific Plan (discussed below), collaborating with the ESCC to develop and prioritize security programs and initiatives.⁴⁵

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

- The **Electricity Sector Information Sharing and Analysis Center (ES-ISAC)**, established in 1998, is the electricity sector’s primary communications channel for security-related information, situational

awareness, incident management, and coordination.⁴⁶ The ES-ISAC is operated by NERC in collaboration with the DOE and ESCC. Members may anonymously share security-related incident information with the ES-ISAC by means of a secure Internet portal. Registered users receive information on security threats and alerts, remediation, task forces, events, and other security-specific resources.⁴⁷

- NERC's **Critical Infrastructure Protection Committee (CIPC)** coordinates NERC's security initiatives and advises NERC's Board of Trustees, its standing physical and cybersecurity committees, and the ES-ISAC. One of the CIPC's key functions is developing, reviewing, and revising security guidelines; and assisting in the development and implementation of NERC standards.⁴⁸
- In January 2015, NERC chartered the **Physical Security Advisory Group (PSAG)**—consisting of representatives from the electric power industry, DOE, DHS, and informed observers—to assist the ES-ISAC in the analysis of physical security threats. The PSAG is intended to offer advice on security plans, policy and procedure, security technology, training, incident response, and threat mitigation strategy to enhance grid physical security and reliability.⁴⁹

DOE's Energy Sector-Specific Plan

The 2006 *National Infrastructure Protection Plan* required each critical infrastructure sector to develop a Sector-Specific Plan (SSP) that describes strategies to protect its critical infrastructure, outlines a coordinated approach to strengthen its security efforts, and determines appropriate funding for these activities. The section of the DOE's *Energy Sector-Specific Plan* addressing electricity was developed in collaboration with the ESCC and EGCC. The plan identifies high-voltage transformers as an electric sector vulnerability due to their criticality to the power grid and the difficulty of replacing them in the event of a successful attack. Among other measures, the SSP established a goal of implementing "agreements that require participants to maintain transformers for possible sharing in the event of a terrorist act."⁵⁰ The plan also identified the "need for a new type of emergency spare (recovery/mobile) high-voltage transformer that can be deployed and energized quickly to rapidly recover from outages caused by natural disasters and deliberate attacks."⁵¹

ESCC's Critical Infrastructure Strategic Roadmap

In November 2010, the Electricity Subsector Coordinating Council published its *Critical Infrastructure Strategic Roadmap* report, to provide a framework for identifying risks that could seriously disrupt the grid and for promoting actions to enhance grid reliability and resilience. The report paid particular attention to “severe-impact risks with the potential to impact large portions of the grid, or disrupt service for an extended period of time.”⁵² The report considered three principal risk scenarios, the first of which relates to physical attacks:

Scenario 1: Physical Attack on Significant Electricity System Equipment

A coordinated physical attack on key nodes of the bulk power system critically disables difficult to replace equipment in multiple generating stations or substations and could have a significant affect [sic] on the remainder of the system. A prolonged period of time is required to fully restore the bulk power system to normal operation.⁵³

The report recommended an assessment of current capability to prevent and respond to such a scenario as a “high priority.” The report also recommended as “important” both a study of “options and practices to enhance physical protection of critical equipment requiring long recovery times (e.g., large high-voltage transformers)” and an initiative to “enhance the availability of critical spare equipment ... starting with high voltage transformers.”⁵⁴

EEI's Threat Scenario Project

In 2011, the Edison Electric Institute (EEI), the main trade association for U.S. investor-owned electric utilities, initiated its Threat Scenario Project to identify security threats and practices utilities could take to mitigate these threats. While the project examined a wide range of potential threats, it included consideration of coordinated physical and cyberattacks.⁵⁵ According to EEI, “the project established common elements for each threat scenario, including a description, likely targets, potential threat actors, specific attack paths, and likely impacts of a successful attack.”⁵⁶ The project is ongoing, with the goal of helping electric utilities “quickly identify areas where security measures are sufficient and where gaps may exist, and begin the dialogue

about additional measures that can be taken to help detect, protect against, respond to, and recover from a range of potential threat scenarios.”⁵⁷

DOE’s Quadrennial Energy Review

As stated above, in April 2015, the DOE released its first *Quadrennial Energy Review* (QER), focusing on energy infrastructure, including “resilience, reliability, safety, and asset security for the electric grid.”⁵⁸ Among its considerations related to the electric grid, the report focuses specifically on the security of HV transformers.

The Administration has made it a priority to work with industry to identify challenges and create solutions for increasing the security and resilience of the electric grid, including the development of an integrated national plan to mitigate challenges pertaining to aging power transformers, the cyber and physical security of transformers, and the vulnerabilities of large power transformers. The Administration is working with trade association leadership and the private sector to improve the coordination of existing and planned transformer-sharing programs and to identify solutions for transformer replacement capabilities as part of its efforts to enhance the resilience of the Nation’s electric grid.⁵⁹

The QER also specifically recommended that DOE should lead a multi-agency (federal and state) and industry initiative to mitigate the risks of HV transformer losses, including the development of additional transformer reserves as discussed below.⁶⁰

Transformer Equipment Programs

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

DHS Recovery Transformer Program

In 2008, the Department of Homeland Security (DHS) initiated a program to develop a prototype “Recovery Transformer” (RecX) which could enable

recovery from transformer failure within days rather than months or longer.⁶¹ The RecX transformer was intended to be adaptable to a range of common grid specifications as well as being smaller, lighter, easier to transport, and quicker to install than conventional HV transformers. The RecX prototype was designed to replace the most common HV transformers (345 kV) used in the U.S. grid.⁶² This design reportedly could be used to replace approximately one quarter of the 2,100 transformers in this voltage class currently deployed.⁶³ In 2012, the only three single-phase RecX prototype units were installed in an operating 345 kV substation in Texas during a simulated emergency drill, where they remain in regular operation, having met or exceeded their service requirements.⁶⁴ The RecX transformers have reliability and efficiency characteristics comparable to other 345 kV transformers, and are also comparably priced (\$7.5 million each).⁶⁵ Although the manufacturer has received no orders for commercial production of these units as of May 2015, a few utilities have expressed interest in leveraging the concepts demonstrated by the RecX program for their own applications.⁶⁶ Having successfully demonstrated the RecX concept, the DHS is no longer funding the RecX program, but the manufacturer has discussed continued development of the concept including higher kV ratings and “hardened” designs.⁶⁷

EEI Spare Transformer Equipment Program

In 2006, the Edison Electric Institute initiated its Spare Transformer Equipment Program (STEP) to strengthen “the sector’s ability to restore the nation’s transmission system more quickly in the event of a terrorist attack.”⁶⁸ The STEP program requires participating utilities to maintain (or acquire) a specific number of transformers up to 500 kV to be made available to other utilities in case of a critical substation failure. Sharing of transformers is mandatory based on a binding contract subject to a “triggering event”—a coordinated act of deliberate, documented terrorism resulting in the destruction or disabling of a transmission substation and the declaration of a state of emergency by the President.⁶⁹ FERC granted blanket authorization for the transfer and cost recovery of transmission equipment under the STEP program in September 2006.⁷⁰ State regulators with jurisdiction over participating utilities have also granted pre-approval for STEP transfers.⁷¹ The program is designed to deal with terrorist events, but it also provides a mechanism for voluntary sharing of transformers in other emergencies, although these may require additional regulatory approvals. EEI requires annual recertification and conducts a STEP program drill every summer to ensure the program and its

members will be fully prepared to respond in the event of an actual triggering event.⁷²

NERC Spare Equipment Database

In 2012, NERC initiated its Spare Equipment Database (SED) program intended to serve as a tool to “facilitate timely communications between those needing long-lead time equipment damaged in a [high impact, low frequency] event and those equipment owners who may be able to share existing equipment being held as spares by their organization.”⁷³ The SED program is a confidential web-based catalog of spare transformers rated at 100 kV or higher. Only NERC and the equipment owners can see their spares data (although NERC can make high-level reports to FERC); requests for equipment disclose neither the requester nor provider (double-blind). Participation is voluntary and requires no commitment or mandatory sharing of spares.⁷⁴ Unlike EEI’s STEP program, however, the SED program has not been granted pre-approval from FERC or state regulators for equipment transfers. Thus, the ability to transfer the ownership of transformers from one company to another may require additional approvals, even during an emergency.

QER Transformer Reserve Proposal

The DOE’s *Quadrennial Energy Review* states that the inventory of HV transformers under EEI’s STEP program is too small to respond to a large, coordinated attack against critical substations, and that transformer design variations and logistics further limit the effectiveness of EEI’s program.⁷⁵ Accordingly, the QER recommends a DOE-led effort to develop one or more HV transformer reserves through a staged process involving: assessment of technical specifications for reserve transformers, where to locate transformers, how many would be needed, how they would be secured and maintained, how they might be transported, and whether new federal authorities or cost sharing would be necessary.⁷⁶ Consistent with this recommendation, a House bill to establish a Strategic Transformer Reserve program (H.R. 2244) introduced on May 8, 2015, would require the Secretary of Energy to submit to Congress “a plan to establish a Strategic Transformer Reserve for the storage, in strategically located facilities, of spare large power transformers in sufficient numbers to temporarily replace critically damaged large power transformers” (Sec. 1(c)(1)). Implementation and funding of such a plan would be subject to congressional approval.

Grid Assurance LLC

On June 10, 2015, a group of eight electric utilities and energy companies⁷⁷ announced a new private sector joint venture company called Grid Assurance “to provide improved responses to major events affecting the electric transmission grid by giving transmission-owning entities access to domestically warehoused long lead-time critical equipment,” including HV transformers.⁷⁸ Grid Assurance would function as a service company open to other transmission companies via a standardized subscriber agreement. Subscription would be voluntary. In an associated filing with FERC, Grid Assurance states that it will

- 1) maintain an optimized inventory of critical spare transformers, circuit breakers and related transmission equipment,
- 2) provide secure domestic warehousing of the inventory of spares in strategic locations, and
- 3) release spare equipment to utility subscribers as needed to respond to emergencies.⁷⁹

The company believes its services will be complementary to, but significantly broader than, EEI’s Spare Transformer Equipment Program. It will offer transformers in a wider range of voltage classes, other long-lead time equipment (e.g., circuit breakers, phase angle regulators, temporary towers), and greater logistical support, among other services.⁸⁰ Grid Assurance has petitioned FERC for a declaratory order affirming that contracting with the company would be permissible as part of a physical security plan under NERC physical security regulations (discussed below), and that acquisition of equipment by utility subscribers from Grid Assurance would not require authorization under Section 203 of the Federal Power Act.⁸¹

Grid Security Exercises and Simulations

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

GridEx and GridEx II

In 2011, NERC conducted GridEx 2011, its first electric sector-wide grid security exercise. The exercise assessed the readiness of utilities to respond to a cyberattack, strengthened their crisis response, and provided input for internal security program improvements. Although the exercise was focused on a cyberattack, it did involve physical incursions into power grid substations as well as aspects of grid monitoring and recovery that would be relevant to an attack on HV transformers.⁸² Among other findings, the exercise determined that “utilities took appropriate steps to secure the grid.”⁸³ Nonetheless, NERC recommended that “entities should ensure their response protocols address a coordinated threat,” and that it would “facilitate and support the development of updated physical security guidance.”⁸⁴

After the Metcalf attack in 2013, NERC conducted a second, more expansive grid security exercise, GridEx II. The exercise scenario, developed using open-source techniques, included a cyberattack on the grid coupled with a coordinated physical attack against a subset of transmission and generation assets—including HV transformer substations.⁸⁵ Among other conclusions, NERC’s after-action report stated:

While the electricity industry has experienced occasional acts of sabotage or vandalism, a well-coordinated physical attack also presents particular challenges for how the industry restores power.... The extreme challenges posed by the Severe Event scenario provided an opportunity for participants to discuss how the electricity industry’s mutual aid arrangements and inventories of critical spare equipment may need to be enhanced.⁸⁶

NERC did not publicly report details about the overall impacts to the grid or outages in particular regions due to the sensitive nature of such information. Utilities and other agencies participating in the exercise viewed it a useful tool for utilities to test their readiness and preparedness for attacks on the grid.⁸⁷ NERC is in the process of preparing for GridExIII to be conducted in November 2015.

FERC “Electrically Significant Locations” Study

In early 2013, prior to the Metcalf attack, then-FERC Chairman John Wellinghoff directed FERC staff to prepare an analysis identifying critical HV substations in the North American power grid.⁸⁸ Using power flow analysis software to model the impacts to the transmission system from the loss of

specific grid assets,⁸⁹ FERC staff compiled a list of “Electrically Significant Locations (ESLs)” within the grid.⁹⁰ Neither details of the ESL study methodology nor its results have been released publicly by FERC or other agencies, although some findings have been reported in the press and discussed publicly by federal officials. According to the *Wall Street Journal*, the FERC analysis identified 30 critical transformer substations; in FERC’s simulation, losing nine of these substations (in various combinations) as the result of a coordinated attack reportedly was found to cause a nationwide blackout for an extended time.⁹¹ As noted above, however, DOE officials have questioned the validity of FERC’s analysis.

Members of Congress were highly critical of both the *Wall Street Journal* and FERC officials for inappropriately releasing what was perceived to be highly sensitive information about power grid physical vulnerability.⁹² The study was not initially designated as security sensitive by commission staff. A subsequent investigation by the Department of Energy’s Inspector General concluded that FERC’s handling of the ESL study findings was improper.⁹³ The protection of information about grid security is further discussed in a later section of this report.

HV Transformer Security Standards

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

IEEE Substation Security Standard

In 2000, the Institute of Electrical and Electronics Engineers (IEEE), a technical professional society, published its first standards for electric power substation physical and electronic security. The voluntary standard addressed “security issues related to human intrusion upon electric power supply substations” and various methods to mitigate them.⁹⁴ The original standard, and subsequent revisions, call for the development of security assessments and, for “high-risk areas,” increased security measures such as motion detectors, perimeter/area detection systems, security cameras, physical

barriers, and posted guards.⁹⁵ However, according to the IEEE, the standard is intended to address security issues related to unauthorized access, theft, and vandalism. The IEEE states that “attacks against the substation for the purpose of destroying its capability to operate, such as explosives, projectiles, vehicles, etc. are beyond the scope of this standard.”⁹⁶

NERC Physical Security Guidance

In June 2002, NERC published its initial guidance for physical response to security alerts from the federal government. This alert system was revised in October 2002 to correspond to DHS’s new color-coded threat level system.⁹⁷ NERC’s guidance was voluntary, intended to provide “examples of security measures that electric utility organizations may consider taking, based on the Alerts issued.”⁹⁸ NERC’s guidance included 35 specific security measures for the five threat DHS levels. These measures ranged from “occasional” workforce awareness programs and annual security plan reviews during times of low threat (green) to continuous monitoring of critical facilities, potentially with armed guards, during times of highest threat (red).⁹⁹ Along with this guidance, NERC published initial guidelines for vulnerability and risk assessment to help identify critical facilities and countermeasures to mitigate threats.¹⁰⁰

In November 2005, NERC published a third version of its physical security guidelines, to provide “examples of security measures that other electricity sector organizations *should* consider when responding to threat level alerts” [emphasis added].¹⁰¹ Thus, while still voluntary, these measures appear to have been intended as recommendations rather than considerations as stated in the earlier versions. The 2005 document included 55 measures, including new measures and existing measures expanded or described more specifically. New measures during times of low threat included, for example, annual audits of critical facility access programs and identifying critical facility long-term and short-term security measures (e.g., vulnerability assessments and security barriers).¹⁰²

The Energy Policy Act of 2005 (P.L. 109-58) mandated the implementation of electric grid reliability standards under new authority granted to the Federal Energy Regulatory Commission. FERC subsequently designated NERC as the Electric Reliability Organization certified by the commission to establish and enforce reliability standards for the U.S. electric transmission grid, subject to commission review. In 2008, FERC approved NERC’s initial reliability standards for critical infrastructure; however, these standards were developed primarily to address transmission grid cybersecurity,

not physical security.¹⁰³ Subsequent NERC standards have expanded these cybersecurity requirements.

In October 2013, NERC published its most recent revision to its physical security guidance, *Security Guideline for the Electricity Sub-sector: Physical Security Response*, providing to electricity sector members “actions they should consider when responding to the threat alerts” issued by the DHS.¹⁰⁴ Continuing its voluntary (rather than regulatory) approach to physical security, NERC’s guidance states that “each organization decides the risk it can accept and the practices it deems appropriate to manage its risk.”¹⁰⁵ This version of NERC’s guidance lays out 77 distinct security measures corresponding to three levels of threat: (1) Normal Operations/Best Practices, (2) Elevated, and (3) Imminent.

FERC Physical Security Best Practices

In 2013, FERC staff along with staff from the Federal Bureau of Investigation (FBI), DOE, DHS, and NERC participated in a number of meetings with utilities and law enforcement agencies to discuss immediate findings and recommendations stemming from the Metcalf substation attack. As part of these meetings, FERC staff shared with utilities a list of best practices for physical security. Although the list has not been made public, it reportedly included prescriptive security measures (e.g., outward-facing video surveillance) focused on security threats similar to that experienced at the Metcalf substation.¹⁰⁶ In 2014, DHS, in coordination with FERC, the ES-ISAC, NERC, the FBI, and industry experts, convened another series of regional briefings across North America with utilities and law enforcement officials to follow up on the initial outreach regarding substation physical security.¹⁰⁷

NERC Physical Security Regulations

On March 7, 2014, FERC ordered NERC to submit to the commission within 90 days proposed reliability standards requiring certain transmission owners “to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation” of the power grid.¹⁰⁸ In its order FERC stated that physical security standards were necessary because “the current Reliability Standards do not specifically require entities to take steps to reasonably protect against physical security attacks.”¹⁰⁹ According to FERC’s order, the new reliability standards were to require transmission owners or operators to perform a risk assessment of their systems to identify their “critical facilities,” evaluate the potential threats and

vulnerabilities to those identified facilities, and develop and implement a security plan designed to protect against attacks to those identified critical facilities.¹¹⁰ The order required that each of these steps be verified by NERC or another third party qualified to review them.

On May 23, 2014, NERC filed with FERC its proposal for mandatory physical security standards.¹¹¹ On November 20, 2014, FERC approved the proposed standard, with minor changes, as NERC's new Physical Security Reliability Standard (CIP-014-1).¹¹² The standard applies to transmission owners with assets operating at 500 kV or higher as well as owners with substations operating between 200 kV and 499 kV if they meet certain interconnection or load-carrying criteria.¹¹³ The standard consists of six principal requirements (R1-R6), summarized as follows:

- R1. Risk assessments by transmission owners to identify critical transmission facilities;
- R2. Independent third party verification of risk assessments conducted under R1;
- R3. Requirement for transmission owners with critical facilities identified under R1 but not under their operational control to notify the transmission operator of these facilities;¹¹⁴
- R4. Mandatory threat and vulnerability assessments for critical facilities conducted by transmission owners and operators;
- R5. Development, documentation, and implementation of physical security plans to protect critical facilities; and
- R6. Independent third party review of the threat and vulnerability assessments performed under R4 and security plans developed under R5.¹¹⁵

The standard also lays out a process for compliance monitoring and assessment including audits, self-certifications, spot checking, violation investigations, self-reporting, and handling complaints.¹¹⁶ The new standard will be enforced by NERC or another Regional Entity under a penalty review policy for mandatory reliability standards approved by FERC subject to the Commission's enforcement authority and oversight under P.L. 109-58.¹¹⁷ According to NERC, the CIP-014-1 physical security standard has staggered enforcement dates with compliance obligations beginning on October 1, 2015.¹¹⁸

Company-Specific Initiatives

Electric utilities have long had an ongoing responsibility to ensure grid reliability, in part through operating practices and investments related to grid safety and security.¹¹⁹ As the standards discussed in the previous section suggest, there has been some level of physical security investment and an increasing refinement of grid security practices across the electric power sector for at least the last 15 years. Nonetheless, several major transmission owners have announced significant new investment initiatives specifically to improve the physical security of critical transformer substations in light of the Metcalf attack. Other utilities have included new substation security investments in broader initiatives for company security.¹²⁰ The following examples illustrate the types of security changes announced by these grid owners. Note that other major utilities have not publicly announced similar new security initiatives, or have kept the details of their security initiatives confidential. A comprehensive review or comparison of physical security plans among all major grid owners in the United States is beyond the scope of this report.

The Tennessee Valley Authority

In February 2012, the Tennessee Valley Authority (TVA) announced that it was “realigning its operations and structure to enhance security at TVA’s non-nuclear power facilities ... focusing more of our non-nuclear security resources on our critical infrastructure,” including HV substations.¹²¹ The realignment included ending uniformed patrols in favor of installing more security technology, and the stationing of contract guards 24 hours a day at critical facilities. Together with local law enforcement cooperation, the shift to contract guards was intended to provide a more persistent security presence and faster incident response at key locations. Among the security technologies reportedly deployed by TVA are “surveillance, infrared cameras, video analytics for alarm verification and assessment, virtual perimeters, card readers, [and] automated gates.”¹²² TVA’s security initiatives in 2012 appear to have been motivated primarily by security concerns such as copper theft, but would be applicable to more serious security risks such as terror attacks.

In February 2014, after the Metcalf incident, TVA reportedly stated that it was “intensifying efforts” to educate local law enforcement about the importance of substations, including taking police on site visits to see substations during normal operations.¹²³ The utility also began canvassing residents near TVA property asking them to report unusual activity around grid facilities. TVA officials have not publicly released details of the

authority's physical security program, but the authority reportedly "takes significant steps, both physically and procedurally, to protect its transmission infrastructure," employing "several layers of protection."¹²⁴ TVA's *Budget Proposal and Management Agenda* for FY2016 discusses \$25 million to \$35 million in cybersecurity investments but does not discuss investments specifically for physical security.¹²⁵ The authority's quarterly report states that "TVA continues to evaluate measures that may be required for compliance" with FERC's new physical security standard "but costs cannot be estimated at this time."¹²⁶

Pacific Gas and Electric (PG&E)

In February 2014, in response to the attack on its Metcalf substation, PG&E announced that it would be investing approximately \$100 million over three years to improve substation security. Physical security measures mentioned by the company included new perimeter barriers, shielding for certain equipment, more cameras (inside and outside the fence), and clearing vegetation. For its most critical facilities, the company was "studying advanced detection technology such as night vision and thermal imaging."¹²⁷ Other security measures mentioned in news reports about PG&E included enhanced lighting, 24-hour security guards, and increased patrols by local law enforcement agencies.¹²⁸ Initial implementation of these measures was inadequate, however, as the Metcalf substation experienced another significant security incident in August 2014, during which thieves breached a perimeter fence and stole several pieces of construction equipment. According to PG&E, human error was a factor because "fence detection alarms received in security operations were not appropriately addressed."¹²⁹

Dominion

In February 2014, Dominion Virginia Power, an operating company of Dominion, announced plans to spend up to \$500 million over five to seven years "to harden its transmission substations and other critical infrastructure against man-made physical threats and natural disasters, as well as stockpile crucial equipment for major damage recovery."¹³⁰ Dominion reportedly began to increase substation security efforts in 2013, focusing first on substations at greatest risk.¹³¹ Among the security measures identified by the utility are physical barriers, additional access control, equipment design/hardening, polymer bushing installation, additional spare equipment, and relocation of spare equipment to off-site storage areas. Other measures reportedly include dual-perimeter "no man zones" around substations and installing systems for

key-card access to substation yards.¹³² As of February 2015, Dominion had begun implementing a series of new physical measures including new risk assessment models, modifications to substation equipment, and improved off-site monitoring.¹³³

Bonneville Power Administration

In its 2014 draft *Security Asset Management Strategy*, the Bonneville Power Administration (BPA) proposed approximately \$37 million in additional capital spending through FY2020 for physical security measures at approximately 60 critical transformer substations.¹³⁴ BPA's *Strategy* stated that, over the prior 13 years, the utility had "conducted hundreds of security and risk assessments using several industry accepted methodologies," and began implementing security improvements based on these risk assessments beginning in 2001.¹³⁵ The administration's 2015 "2nd Quarter Capital Project Status Report" includes \$49.9 million in capital spending to acquire five 500 kV spares and relocate two existing transformers to be used as spares placed strategically across the BPA system.¹³⁶ BPA has 105 single-phase transformers (35 banks) rated at 500kV in service.¹³⁷

New York Power Authority

The New York Power Authority (NYPA) in January 2015 requested authorization from its trustees for \$42.5 million in capital expenditures primarily for physical security upgrades at critical substation in its transmission system.¹³⁸ Planned upgrades include fence intrusion detection systems, modification of physical security perimeters, installing key card access systems, surveillance cameras, laser detection systems, and associated control and monitoring systems, among other measures.¹³⁹

Pepco Holdings

In May 2014, Pepco Holdings reportedly announced a \$40 million project to upgrade physical security at various substations in the company's transmission system.¹⁴⁰ The company states that it has established a physical security working group, has conducted on-site physical security assessments, and has been collaborating with other entities to focus on the best security improvement opportunities. Pepco's physical security measures include guarded facilities for spare equipment, enclosing substations, improving communications connectivity, maintaining spare equipment, and considering physical security when evaluating new facilities.¹⁴¹

ISSUES FOR CONGRESS

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

Identifying Critical Transformers

A fundamental consideration regarding HV transformer security is a clear and stable understanding of which transformers are “critical.” The USA PATRIOT Act of 2001 defines “critical infrastructure” in the most general sense as “systems and assets ... so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”¹⁴² In its 2009 guidelines for identifying critical assets specifically in the electricity sector, NERC defines critical assets as those “that if destroyed, degraded, compromised (e.g., misused) or otherwise rendered unavailable would unacceptably affect the reliability or operability of the [bulk-power system] as a whole....”¹⁴³ FERC’s 2014 order mandating physical security standards for the grid defines a “critical facility” as “one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System.”¹⁴⁴ All three definitions associate “criticality” with a failure event of national significance, although none provides a more prescriptive basis for identifying such assets.

In its physical security order, FERC does not require that a “mandatory” number of critical facilities be identified under the standards.¹⁴⁵ Determination of whether a specific HV transformer is “critical” will be based on each individual asset owner’s “objective analysis, technical expertise, and experienced judgment.”¹⁴⁶ In its physical security standards, NERC requires transmission owners with HV assets meeting prescriptive criteria to examine whether they *may* have critical transformers, but it is up to the owners to determine themselves if any of their assets *are* critical through a periodic risk assessment based on their own respective transmission analyses, subject to independent validation.¹⁴⁷ Thus, grid owners could have considerable latitude

in determining which of their transformer substations (if any) are critical and therefore subject to the requirements of the new standard.

Although there are many candidate transformer substations in the grid, relatively few are likely to be of national significance. As discussed above, of the numerous HV transformer substations in the United States, FERC's 2013 power flow analysis identified only 30 as being critical to the national grid (although each of these substations may contain multiple HV transformers). Whether the number of critical transformer substations under FERC's definition above turns out to be higher or lower than 30, it will likely be only a small fraction of the total asset base. This conclusion is consistent with FERC's expectation that under NERC's new standard "the number of facilities identified as critical will be relatively small.... For example, of the many substations on the Bulk-Power System, our preliminary view is that most of these would not be 'critical' as the term is used in this order."¹⁴⁸ Consistent with this view, the NERC working group responsible for drafting the proposed physical security standard likewise expected the number of critical facilities to be "small and that many Transmission Owners that meet the applicability of this standard will not actually identify any such Facilities."¹⁴⁹

Although the new NERC physical security standards were approved by FERC after extensive utility and public comments, some stakeholders take issue with specific requirements and methodology in the standards. For example, some analysts have objected to NERC's standards as focusing too narrowly on a limited number of substations evaluated individually. They argue this approach fails to adequately consider potential impacts from a planned, multi-substation attack. They assert that NERC's approach may overlook transformers that are "critical" in the context of such an attack.¹⁵⁰ FERC has rejected these arguments (for the time being) arguing that "by protecting individual critical facilities, responsible entities will necessarily protect critical facilities against simultaneous attacks."¹⁵¹ FERC states that it is not prepared "to expand the scope of covered facilities to include those not individually critical ... at this early stage of industry experience with the new requirements. Our priority at this time is to have responsible entities protect the most critical facilities."¹⁵² However, the commission also states that it remains "open to a different approach in the future as industry continues to gain experience in this area and as risks may evolve."¹⁵³

Properly identifying which HV transformer substations are critical is a key issue. Otherwise, the electricity sector risks the possibility of hardening too many substations, hardening the wrong substations, or both. Either outcome could increase ultimate costs to electricity consumers without commensurate

security benefits, and could potentially divert limited security resources from other important grid priorities (e.g., cybersecurity). Hardening too few substations could leave the grid exposed to unacceptable levels of risk. Independent verification is intended to validate utility assessments of substation criticality, but the standard's reliance on company-by-company assessments may still allow for important differences in analytic methodology or assumptions, and thus inconsistent conclusions about transformer criticality. Furthermore, company-specific studies may not align with a "top down" assessment of asset criticality like that performed by FERC in its Electrically Significant Location (ESL) analysis. Congress may examine whether company-specific assessments of transformer criticality could differ from national-level assessments or assessments using other analytic approaches, and what implications, if any, such differences might have on overall grid security and company efforts to protect particular substations.

Confidentiality of Critical Transformer Information

Ensuring the confidentiality of critical infrastructure information has been a long-standing concern across all critical infrastructure sectors. It is a key reason for the establishment of sector Information Sharing and Analysis Centers (ISACs), including the Electricity Sector ISAC, discussed above. Confidentiality also factors into the administration of the industry's spare transformer programs and other activities related to critical infrastructure. FERC has established policies for the protection of critical energy infrastructure information (CEII) through a series of orders, beginning with Order 630, issued February 21, 2003.¹⁵⁴ The order (§27) defines CEII as information that "must relate to critical infrastructure, be potentially useful to terrorists, and be exempt from disclosure under the Freedom of Information Act [FOIA]." It also establishes procedures and responsibilities for determining what information qualifies as CEII and handling CEII requests.¹⁵⁵ FERC's 2014 order mandating physical security standards also requires procedures to ensure confidential treatment of sensitive information.¹⁵⁶

Press articles in the wake of the Metcalf attacks, notably in the *Wall Street Journal*, cited specific details about FERC's 2013 ESL analysis, reportedly from a copy of a FERC presentation obtained by the paper. Notwithstanding FERC's orders on CEII, Members of Congress and FERC officials have expressed concern that the release of the presentation by FERC staff and the publication of details in the press potentially compromised grid security.¹⁵⁷

Others reportedly have disputed this concern, including the former FERC Commissioner responsible for commissioning and presenting the ESL study findings at industry meetings.¹⁵⁸ In April 2014, the DOE Inspector General issued a management alert which concluded that the FERC presentation in question “should have been classified and protected from release” and “that the Commission may not possess adequate controls for identifying and handling classified national security information.”¹⁵⁹ The Acting Chairman of FERC testified at the time that the commission was adopting the Inspector General’s recommendations to improve its handling of CEII and requested additional authority from Congress for exemption from FOIA.¹⁶⁰

On January 30, 2015, the DOE Inspector General released a follow up inspection report related to the IG’s earlier examination of CEII handling by FERC. The report concluded that

the Commission’s controls, processes and procedures for protecting nonpublic information were severely lacking. Specifically, we found that staff inconsistently handled and shared Commission-created analyses that identified vulnerability of the Nation’s electric grid without ensuring that the data was adequately evaluated for sensitivity and classification.¹⁶¹

The IG report noted that FERC’s actions to remediate its CEII lapses since the IG’s earlier Management Alert were “a good start,” but that additional measures were recommended.¹⁶²

According to the IG, FERC’s comments and additional plans in response to the new report were generally responsive to the report’s findings and recommendations.¹⁶³

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

The Critical Electric Infrastructure Protection Act (H.R. 2271 §2(a)) would strengthen federal protections for critical electric infrastructure information. Among other provisions, the bill would exempt such information from disclosure under the Freedom of Information Act or any state, tribal, or local law requiring such disclosure. The bill would also require FERC to promulgate regulations, issue orders, provide standards, and specify sanctions to ensure appropriate sharing of critical electric infrastructure information and prevent its unauthorized release. The bill would allow federal officials to grant temporary access to classified information to key personnel of entities subject to grid security emergency measures, further discussed below.

Adequacy of HV Transformer Protection

The electric power sector has had physical security guidelines in place for well over a decade, as discussed above. These voluntary guidelines have been updated and expanded periodically to reflect industry experience, changes in the security environment, and new technologies. Prior to 2014, however, it appears that the physical security initiatives among grid owners were focused primarily on preventing vandalism and theft (of copper wire) rather than a terrorist attack.¹⁶⁴ As the recent substation attacks in California, Arkansas, and Florida have shown, many other security measures available to grid owners were not implemented—even at critical HV substations.

A grid owner's focus on vandalism and theft may be understandable because such incidents have occurred frequently and their associated costs are tangible and well-understood. Investing in security against a terrorist attack presents a greater challenge in terms of costs and benefits. As a 2006 report from the Electric Power Research Institute states,

Security measures, in themselves, are cost items, with no direct monetary return. The benefits are in the avoided costs of potential attacks whose probability is generally not known. This makes cost-justification very difficult.¹⁶⁵

Note that cost-justification requires not only the approval of utility management, but also of FERC and potentially state public utility commissions which regulate the rates grid owners may charge for electric transmission and distribution service. Regulators are responsible for ensuring that electricity rates are just and reasonable. They must be convinced that any

new grid security capital costs and expenses are necessary and prudent before they will allow them to be passed through to ratepayers.¹⁶⁶

The Metcalf incident and GridEx exercises have provided the electric sector with valuable new information about the potential threat, vulnerability, and consequence of a coordinated attack on HV transformers. Risk assessments incorporating this information presumably would justify (with or without a new NERC standard) increased security investments at critical substations to prevent intentional attacks. The spending plans announced in 2014-2015 at PG&E, Dominion, BPA, and other utilities for HV substation security appear to reflect such risk and cost-benefit reassessments. Nonetheless, there continues to be considerable uncertainty about the risk of terror attacks on the power grid, and what measures are economically justified in addressing them. PG&E, BPA, and the other utilities announcing large security investments have already decided to make such investments. Other major owners of critical HV transformers have not publicly announced similar plans, in some cases because they have not yet completed security evaluations under NERC's new standards, so they are unsure what new measures they will require. For example, based upon a security gap analysis after the Metcalf incident, Florida Power and Light (FPL) identified multiple potential security enhancements, but has only implemented some of them; other measures have been delayed for comparison to requirements under NERC's new standards.¹⁶⁷

NERC's proposed standards for power grid physical security would ensure considerable consistency in the *analytic process* utilities must undertake to identify critical substations and develop plans to secure them. However, the standard may not ensure consistency among the various security plans nor in the specific measures the individual asset owners will choose to implement to reduce the risk of intentional attacks. Apart from the physical aspects of their assets, a number of factors may lead to differences in security implementation among grid owners, including differences in organization, ratemaking, accounting, and management capability. In particular, how physical security is managed within a corporate structure can influence the effectiveness of physical security programs. For example, a 2014 corporate memo from PG&E leaked to the press states that "due to the existing structure and limited authority of CSD [Corporate Security Division], little has changed relative CSD's abilities to make significant and intended security improvements."¹⁶⁸ How capital is allocated and accounted for can also be a barrier to physical security implementation and verification. In a 2014 report to Florida regulators, FPL stated that

not all security costs are contained within the Corporate Security budget. Some physical security costs are shared with appropriate operational business units. For example, the cost of security equipment for new substations is rolled into the cost of the substation. Not all physical security costs are budgeted and tracked in separate line items. Therefore, difficulties exist estimating total costs of FPL's physical security efforts.¹⁶⁹

As FERC continues to implement its policy of regulating physical security of the power grid, Congress may examine whether company-specific security initiatives appropriately reflect the risk profiles of their particular assets, and whether additional security measures across the grid uniformly reflect terrorism risk from a national perspective. Examining the extent to which the corporate structures and accounting functions support company-specific physical security programs may be of particular interest as grid owners adapt to evolving threats and physical security requirements.

Quality of Federal Threat Information

The power industry's physical security risk assessments rely upon information about security threats provided by the federal government, among other sources, communicated through the ISAC, during DHS and other agency briefings, or through other channels. The quality and timeliness of this threat information is a key determinant of what grid owners need to be protecting against and what security measures to take. Incomplete or ambiguous threat information—especially from the federal government—may lead to inconsistency in physical security among grid owners, inefficient spending of limited security resources at facilities (e.g., that may not really be under threat), or deployment of security measures against the wrong threat. For example, prior to FERC's physical security order, the head of NERC, which initially opposed mandatory physical security standards, stated?

I am concerned that a rule-based approach for physical security would not provide the flexibility needed to deal with the widely varying risk profiles and circumstances across the North American grid and would instead create unnecessary and inefficient regulatory burdens and compliance obligations.¹⁷⁰

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

Concerns about the quality and specificity of federal threat information have long been an issue across all critical infrastructure sectors.¹⁷¹ Threat information continues to be an uncertainty in the case of power grid physical security. For example, the PJM regional transmission organization employs probabilistic models to assess risks to the grid due to equipment malfunction and severe weather, but its model has not incorporated an assessment of a physical attack due to insufficient data.¹⁷²

Some federal officials reportedly have characterized the Metcalf incident as a domestic terrorist attack, potentially a “dry run” for a more destructive attack on multiple HV transformer substations, while the Federal Bureau of Investigation has stated that it does not believe Metcalf was a terrorist incident.¹⁷³ Because the perpetrators have not been identified, it is impossible to know for certain, but the ambiguity has significant implications for HV substation security going forward. Although there is wide consensus that the Metcalf attack was extremely serious, some industry analysts have opined that FERC’s physical security order may be an “overreaction” to Metcalf.¹⁷⁴ By contrast, former DHS Secretary Michael Chertoff has predicted that “the sophistication and resulting damage of the Metcalf attack will ... be exceeded” in a future attack.¹⁷⁵ Still others have expressed concern that FERC’s physical security concerns may be too heavily focused on another Metcalf-type scenario (the last threat) rather than a wider range of potential future threats (the next threat).¹⁷⁶

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

by grid owners, and how limitations and uncertainty of this information may affect the HV transformer physical security among electric utilities.

Recovery from HV Transformer Attacks

Physical security for HV transformer substations has the primary purpose of preventing successful attacks against these critical assets within the power grid. However, in the event of a successful attack, measures to minimize its effect on the overall grid are equally important so that the loss of any particular transformer remains a local event. To this end the electric power industry emphasizes its strategy of “defense-in-depth,” which includes incident response and recovery in addition to preparation and prevention.¹⁷⁷ Industry initiatives to enhance grid resiliency, including incident recovery programs such as the DHS recovery transformer program and EEI’s spare transformer program, contribute to the power grid’s ability to sustain a terrorist attack without widespread grid failure. Indeed, some analysts have pointed to the Metcalf incident as a successful demonstration of grid resiliency; electric service was not interrupted despite the loss of a critical substation in the San Francisco Bay area. Nonetheless, some policymakers have proposed additional federal authorities to respond to physical incidents affecting grid critical infrastructure, including HV transformers.

Some stakeholders, including FERC officials, have asserted that the commission’s current grid reliability authority under the Federal Power Act (§215) does not provide FERC with adequate authority for emergency action in the event of an attack on the grid. A House bill to amend the Federal Power Act with respect to critical electric infrastructure security (H.R. 2271) would allow the President to authorize the Secretary of Energy to order emergency measures to protect grid reliability during a “grid security emergency” (§(b)(1)). The director of FERC’s electric reliability office has testified in support of the bill that FERC’s existing “procedures ... for the development and approval of reliability standards do not provide an effective and timely means of addressing urgent cyber or other national security risks to the bulk power system.”¹⁷⁸ NERC’s president likewise has testified that he generally supports legislation clarifying federal authority during grid emergencies, as long as they focus clearly on “national, catastrophic instances” and do not conflict with the existing system of ongoing measures in place to protect the grid.¹⁷⁹ Utility industry representatives also support facilitation of industry-government coordination in the event of an attack on the grid.¹⁸⁰ As

consideration of H.R. 2271 or similar legislation continues, Congress may focus on specific language related to consultation, duration of emergency measures, grid recovery activities, and other details to ensure that they align with a complex industry structure while achieving the bill's objectives in the event of a future security incident.

As discussed above, the DOE's *Quadrennial Energy Review* calls for federal efforts to develop one or more critical HV transformer reserves. H.R. 2244 would mandate a DOE plan for how such a reserve program could be carried out. Some in the utility industry support the policy intentions of such a reserve, as already demonstrated by the industry's own spare HV transformer programs and planned expansion of those programs, but they believe stakeholders "will be better served by allowing the industry to create the structure, cost responsibility and pricing for [transformer] sparing services as opposed to a top-down government solution."¹⁸¹ They believe federal assistance would be most helpful if limited to funding the startup of a transformer reserve program administered by the asset owners themselves. The Grid Assurance sparing service appears consistent with a private sector-driven approach to expand existing spare transformer initiatives.

Others have questioned the cost-effectiveness of a new national HV transformer reserve program, asserting that—had it been in place—the reserve program envisioned by H.R. 2244 would not have been called upon by any grid incident over the last ten years.¹⁸² As Congress considers any plans for a federally administered strategic transformer reserve, it may consider the relationship of such a program to ongoing industry efforts to maintain HV transformer spares, the relationship between federal and state administrators of such a program, its cost-effectiveness, and its practical requirements (e.g., size, location, and transportation).

Electric Grid Resilience

In addition to measures focused on the protection of critical HV transformers from physical attack, analysts have advocated policies to reduce the criticality of individual HV assets by enhancing the overall "resiliency" of the electric power grid. As a report from the Executive Office of the President states,

Grid resilience ... includes hardening, advanced capabilities, and recovery/reconstitution. Although most attention is placed on best

practices for hardening, resilience strategies must also consider options to improve grid flexibility and control. Resilience includes reconstitution and general readiness such as pole maintenance, vegetation management, use of mobile transformers and substations, and participation in mutual assistance groups.¹⁸³

A number of federal, state, and industry initiatives exist to address various aspects of electric power grid resiliency. While many of these initiatives have been motivated by weather-related events such as the Northeast Blackout of 2003 and electric grid failure during Superstorm Sandy, policies to improve grid resilience also have benefits in the context of intentional physical attacks. For example, an official from PJM has reportedly stated,

You can only harden a substation so much. If someone wants to attack a substation, they will.... That leads us to the resilience piece. Maybe the best way to make a substation less critical is to build more transmission. A substation is critical basically because we're pushing too much power through it.¹⁸⁴

Grid scale energy storage, distributed generation, smart grid technology, and other measures to redistribute or optimize transmission system power flows may also increase grid resiliency and reduce vulnerability to physical security threats.

The Enhanced Grid Security Act of 2015 (S. 1241) would require the Secretary of Energy develop an advanced energy security program to increase the “functional preservation” of the electric grid in the face of both natural and human-made threats and hazards (§7(b)). The objectives of the program would explicitly include both “security and resiliency” through vulnerability assessment, modeling, exercises, research, and technical assistance (§7(c)). The Grid Modernization Act of 2015 (S. 1243) would likewise encourage greater grid resilience, including modelling, research, and investment in grid modernization and new technologies—including tools to increase physical security (§101(3)(E)). Other legislation related to power grid resilience or efficiency would also likely have physical security implications. As Congress continues its examination of physical security policy, maintaining an integrated perspective on prevention, recovery, and resilience may help to promote an effective balance among industry investment, regulatory requirements, and federal oversight.

End Notes

- ¹ Portions of this report were drawn from CRS Report R42795, *Electric Utility Infrastructure Vulnerabilities: Transformers, Towers, and Terrorism*, by Amy Abel, Paul W. Parfomak, and Dana A. Shea.
- ² 1 kV=1,000 volts.
- ³ North American Electric Reliability Corporation, “Understanding the Grid,” fact sheet, August 2013, <http://www.nerc.com/AboutNERC/Documents/Understanding%20the%20Grid%20AUG13.pdf>. Note that there is no industry consensus as to what voltage rating or other operating characteristic constitutes “high voltage.” This report uses 230 kV as the high voltage threshold, but other studies may use a different threshold, such as 115/138 kV, or may include an additional “extra high voltage” category above 345 kV. See, for example, U.S. Department of Energy, *Large Power Transformers and the U.S. Electric Grid*, April 2014, p. 4.
- ⁴ C. Newton, “The Future of Large Power Transformers,” *Transmission & Distribution World*, September 1, 1997; William Loomis, “Super-Grid Transformer Defense: Risk of Destruction and Defense Strategies,” Presentation to NERC Critical Infrastructure Working Group, Lake Buena Vista, FL, December 10-11, 2001; Electric Power Research Institute (EPRI), *Considerations for a Power Transformer Emergency Spare Strategy for the Electric Utility Industry*, prepared for the U.S. Department of Homeland Security, September 30, 2014, p. 13.
- ⁵ See, for example: Senators Dianne Feinstein, Al Franken, Ron Wyden, and Harry Reid, letter to the Honorable Cheryl LaFleur, Acting Chairman, Federal Energy Regulatory Commission, February 7, 2014, <http://www.ferc.gov/industries/electric/indus-act/reliability/chairman-letter-incoming.pdf>.
- ⁶ The three currents are sine wave functions of time with the same frequency (60 Hertz). The phases are spaced equally, offset 120 degrees from each other. With three-phase power, one of the phases is always nearing a peak.
- ⁷ The loss of power on the transmission system is proportional to the square of the current (flow of electricity) while the current is inversely proportional to the voltage.
- ⁸ Pauwels Canada, Inc., personal communication, October 20, 2003.
- ⁹ U.S. Department of Energy, April 2014, p. 7.
- ¹⁰ U.S. Department of Energy, April 2014, p. 9.
- ¹¹ Emily Heitman, ABB Inc, Testimony before the House Committee on Energy and Commerce, Subcommittee on Energy and Power hearing entitled “Discussion Draft Addressing Energy Reliability and Security,” May 19, 2015; Pauwels Canada, Inc., October 20, 2003.
- ¹² U.S. Department of Energy, April 2014, p. 7.
- ¹³ C. Newton, “The Future of Large Power Transformers,” *Transmission & Distribution World*, September 1, 1997.
- ¹⁴ C. Newton, September 1, 1997.
- ¹⁵ U.S. Department of Energy, April 2014, p. 27.
- ¹⁶ Kenneth Friedman, U.S. Department of Energy, “DOE Update on GMD/EMP-Related Activities,” Presentation to the Geomagnetic Disturbance Task Force Working Group, North American Electric Reliability Corporation, November 13, 2013.
- ¹⁷ John Kappenman, *Geomagnetic Storms and Their Impacts on the U.S. Power Grid*, Meta-R-319, Metatech Corp., prepared for Oak Ridge National Laboratory, January 2010, p. 1-14,

- http://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc_meta-r-319.pdf.
- ¹⁸ HV substation information for specific investor-owned utilities is publicly available in annual reports filed with the Federal Energy Regulatory Commission (FERC Form-1).
 - ¹⁹ National Research Council (NRC), *Terrorism and the Electric Power Delivery System*, 2012, p. 69; EPRI, September 30, 2014, p. 7.
 - ²⁰ Office of Technology Assessment (OTA), *Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage*, OTA-E-453, June 1990, p. 37.
 - ²¹ See, for example, Réka Albert, István Albert, and Gary L. Nakarado, "Structural Vulnerability of the North American Power Grid," *Physical Review E*, Vol. 69, 025103(R), 2004.
 - ²² Rebecca Smith, "U.S. Risks National Blackout From Small-Scale Attack," *Wall Street Journal*, March 12, 2014.
 - ²³ U.S. Department of Energy, Office of Inspector General, *Inspection Report: Review of Controls for Protecting Nonpublic Information at the Federal Energy Regulatory Commission*, DOE/IG-0933, January 2015, p. 5.
 - ²⁴ Rebecca Smith, "Assault on California Power Station Raises Alarm on Potential for Terrorism," *Wall Street Journal*, February 5, 2014.
 - ²⁵ U.S. Department of Energy, *Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure*, April 2015, p. S-11.
 - ²⁶ Mitsubishi Electric Power Products, Inc., personal communication, Warrendale, PA, September 23, 2003.
 - ²⁷ Lower Colorado River Authority, "August 6 Update on Transformer Fire," press release, August 6, 2003.
 - ²⁸ RTO Insider, "Substation Saboteurs 'No Amateurs'," April 2, 2014, <http://www.rtoinsider.com/pjm-grid2020-1113-03/>.
 - ²⁹ Chelsea J. Carter, "Arkansas Man Charged in Connection with Power Grid Sabotage," CNN, October 12, 2013; Max Brantley, "FBI Reports Three Attacks on Power Grid in Lonoke County," *Arkansas Times*, October 7, 2013.
 - ³⁰ Jim Peppard, "Reward Offered in Power Transformer Shooting," WTSP News (Tampa), October 17, 2005.
 - ³¹ David Egan and Kenneth Seiler, PJM Interconnection, "PJM Manages Aging Transformer Fleet," *T&D World*, March 1, 2007.
 - ³² Tom Daspit, "Schnabel Cars in Service," web page, August 15, 2013, http://southern.railfan.net/schnabel/schnabel_cars.html.
 - ³³ U.S. Department of Energy, April 2015, p. S-20.
 - ³⁴ Marija Ilic, Professor, Engineering and Public Policy and Electrical and Computer Engineering, Carnegie Mellon Univ., Pittsburgh, PA, personal communication, September 22, 2003.
 - ³⁵ Critical Intelligence, Inc., "Grid Strike," summary report, Idaho Falls, ID, 2014. The methodology and results of this study were not independently validated; the analysis is proprietary.
 - ³⁶ NRC, 2012, p.79.
 - ³⁷ OTA, June 1990, pg. 37.
 - ³⁸ Stewart Tendler, "IRA Bombers Plotted to Black Out London and South East for Months," *The Times*, London, England, April 12, 1997.
 - ³⁹ Axl Hess (a.k.a. Aquilifer), *White Resistance Manual V2.4*, 2001. See also Herschel Smith, "A Terrorist Attack That America Cannot Absorb," captainsjournal.com, blog, September 28,

- 2010, <http://www.captainsjournal.com/2010/09/28/a-terrorist-attack-that-america-cannot-absorb/>.
- ⁴⁰ Department of Homeland Security (DHS), “National Infrastructure Protection Plan,” web page, April 7, 2014, <https://www.dhs.gov/national-infrastructure-protection-plan>. The NIPP was mandated under Homeland Security Presidential Directive 7 issued on December 17, 2003.
- ⁴¹ Presidential Policy Directive 21, *Presidential Policy Directive—Critical Infrastructure Security and Resilience*, February 12, 2013.
- ⁴² North American Electric Reliability Corporation (NERC), “Electricity Sub-sector Coordinating Council,” web page, April 7, 2014, <http://www.nerc.com/pa/CI/Pages/ESCC.aspx>.
- ⁴³ Among other functions, NERC develops and enforces reliability standards, monitors the grid, and trains industry personnel. In the United States, NERC is subject to Federal Energy Regulatory Commission oversight.
- ⁴⁴ Gerry W. Cauley, North American Electric Reliability Corporation (NERC), letter to U.S. Secretary of Energy Ernest Moniz, August 23, 2013, <http://www.publicpower.org/files/PDFs/DOESecLetterHistoryESCC.pdf>.
- ⁴⁵ Department of Energy, *Energy Sector-Specific Plan*, 2010, p. 20.
- ⁴⁶ The ES-ISAC was established under Presidential Decision Directive 63, May 22, 1998.
- ⁴⁷ Electricity Sector Information Sharing and Analysis Center (ES-ISAC), “Frequently Asked Questions,” web page, <https://www.esisac.com/SitePages/FAQ.aspx>.
- ⁴⁸ North American Electric Reliability Corporation (NERC), “Critical Infrastructure Protection Committee (CIPC),” web page, <http://www.nerc.com/comm/CIPC/Pages/default.aspx>, April 8, 2014.
- ⁴⁹ North American Electric Reliability Corporation, “ES-ISAC Physical Security Advisory Group (PSAG) Charter,” January 20, 2015.
- ⁵⁰ Department of Homeland Security, *Energy Sector-Specific Plan*, 2010, p. 54.
- ⁵¹ Department of Homeland Security, *Energy Sector-Specific Plan*, 2010, p. 70.
- ⁵² North American Electric Reliability Corporation (NERC), *Critical Infrastructure Strategic Roadmap*, November 2010, p. 2, http://ccpic.mai.gov.ro/docs/NERC_ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf.
- ⁵³ NERC, November 2010, p.18. This scenario involved the loss of three HV substations serving large urban centers with a restoration time to 100% operating capacity of 6-18 months.
- ⁵⁴ NERC, November 2010, pp.19-20.
- ⁵⁵ Edison Electric Institute and Chertoff Group, “EEI Business Continuity Conference Threat Scenario Project (TSP),” slide presentation, April 4, 2012, http://www.eei.org/meetings/Meeting_Documents/2012Apr-BusinessContinuity-Treat%20Scenario%20Project_Engels.pdf.
- ⁵⁶ Edison Electric Institute, “Electric Power Industry Initiatives to Protect the Nation’s Grid From Cyber Threats,” fact sheet, January 2013, <http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity%20Industry%20Initiatives.pdf>.
- ⁵⁷ Chertoff Group, “Addressing Dynamic Threats to the Electric Power Grid through Resilience,” November 2014, p. 5.
- ⁵⁸ U.S. Department of Energy, April 2015, p. 2-8.
- ⁵⁹ U.S. Department of Energy, April 2015, p. 2-15.
- ⁶⁰ U.S. Department of Energy, April 2015, p. 2-40.
- ⁶¹ The program was partly funded by the DHS Science and Technology Directorate in a consortium with the Electric Power Research Institute, CenterPoint Energy, and ABB.
- ⁶² ABB, “US Rapid Recovery Transformer Initiative Succeeds Using Specially-Designed ABB Transformers,” press release, October 4, 2012.

- ⁶³ Matthew L. Wald, "A Drill to Replace Crucial Transformers (Not the Hollywood Kind)," *New York Times*, March 14, 2012.
- ⁶⁴ EPRI, September 30, 2014, p. 7.
- ⁶⁵ National Research Council (NRC), *The Resilience of the Electric Power Delivery System in Response to Terrorism and Natural Disasters: Summary of a Workshop*, 2013.
- ⁶⁶ Sarah Mahmood, Department of Homeland Security, personal communication, May 28, 2015.
- ⁶⁷ ABB, "ABB and U.S. Policymakers Meet to Address Grid Vulnerability Issues," press release, May 21, 2015.
- ⁶⁸ Edison Electric Institute (EEI), "Spare Transformers," web page, April 10, 2014, <http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx>.
- ⁶⁹ Edison Electric Institute (EEI), "Overview of the Spare Transformer Equipment Program," slide presentation, February 23, 2014.
- ⁷⁰ Federal Energy Regulatory Commission, *Order on Application for Blanket Authorization for Transfers of Jurisdictional Facilities and Petition for Declaratory Order*, Docket Nos. EC06-14-000 and EL06-86-000, September 22, 2006.
- ⁷¹ EEI, February 23, 2014.
- ⁷² Edison Electric Institute, briefing for the Congressional Research Service, February 23, 2014.
- ⁷³ North American Electric Reliability Corporation (NERC), *Special Report: Spare Equipment Database System*, August 2011.
- ⁷⁴ North American Electric Reliability Corporation (NERC), "Spare Equipment Database," slide presentation, NERC Industry Webinar, July 22, 2013, http://www.nerc.com/pa/RAPA/webinar/SED_Presentation_July_22_2013.pdf.
- ⁷⁵ U.S. Department of Energy, April 2015, p. 2-11.
- ⁷⁶ U.S. Department of Energy, April 2015, p. 2-40.
- ⁷⁷ American Electric Power (AEP), Berkshire Hathaway Energy, Duke Energy, Edison International, Eversource Energy, Exelon, Great Plains Energy, and Southern Company.
- ⁷⁸ Grid Assurance, LLC, "Eight Utilities and Energy Companies Announce Plans for Critical Transmission Equipment Service Company," press release, June 10, 2015, <http://gridassurance.com/lib/docs/Grid%20Assurance%20New%20Release%20FINAL%206-9.pdf>.
- ⁷⁹ Grid Assurance LLC, Petition for Declaratory Order and Request for Expedited Action filed with the Federal Energy Regulatory Commission, Docket No. EL15-, June 9, 2015, p. 1.
- ⁸⁰ Grid Assurance, LLC, June 9, 2015, pp. 20-21.
- ⁸¹ Grid Assurance, LLC, June 9, 2015, pp. 22-23.
- ⁸² North American Electric Reliability Corporation (NERC), *2011 NERC Grid Security Exercise: After Action Report*, March 2012, p. i.
- ⁸³ NERC, 2012, p. ii.
- ⁸⁴ Ibid.
- ⁸⁵ North American Electric Reliability Corporation (NERC), *Grid Security Exercise (GridEx II): After-Action Report*, March 2014, p.15; Matthew L. Wald, "Attack Ravages Power Grid. (Just a Test.)," *New York Times*, November 14, 2013.
- ⁸⁶ NERC, March 2014, p. 5.
- ⁸⁷ See, for example, American Public Power Association, "Physical Security and the Electric Sector," fact sheet, February 2014, <http://www.publicpower.org/files/PDFs/PhysicalSecurityIBFebruary2014.pdf>; Matthew L. Wald, "Power Grid Preparedness Falls Short, Report Says," *New York Times*, March 12, 2014.
- ⁸⁸ Federal Energy Regulatory Commission (FERC), "Second Set of Responses of the Federal Energy Regulatory Commission to Senator Murkowski's Separately Submitted Questions

- for the Record from April 10, 2014 Hearing of the Senate Energy and Natural Resources Committee,” May 5, 2014, pp. 12-13, http://www.energy.senate.gov/public/index.cfm/files/serve?File_id=5c3bf9d7-bb7f-4379-8f57-f58881a0b5d6.
- ⁸⁹ FERC staff employed the commission’s Topological and Impedance Element Ranking (TIER) model to identify “significant” assets based upon undisclosed criteria. For more details of the TIER model, see Bernard C. Lesieutre et al., “Topological and Impedance Element Ranking (TIER) of the Bulk- Power System,” University of Wisconsin— Madison, prepared for the Federal Energy Regulatory Commission, August 2009, <https://www.ferc.gov/EventCalendar/Files/20090911112656-TIER%20REPORT.pdf>.
- ⁹⁰ Federal Energy Regulatory Commission (FERC), “Response to Senator Murkowski’s Separately Submitted Questions for the Record from April 10, 2014 Hearing of the Senate Energy and Natural Resources Committee, Question 39,” May 5, 2014, p. 2, http://www.energy.senate.gov/public/index.cfm/files/serve?File_id=2826f80a-a986-45d1-9261-87b45e1d6872.
- ⁹¹ Rebecca Smith, “U.S. Risks National Blackout from Small-Scale Attack on Substations,” *Wall Street Journal*, March 13, 2014.
- ⁹² Senate Committee on Energy and Natural Resources, “Landrieu, Murkowski Ask Inspector General to Examine Leaks of Grid Vulnerabilities,” press release, March 31, 2014.
- ⁹³ U.S. Department of Energy, Office of Inspector General, “Review of Internal Controls for Protecting Non-Public Information at the Federal Energy Regulatory Commission,” DOE/IG-0906, April 9, 2014.
- ⁹⁴ Institute of Electrical and Electronics Engineers (IEEE), *1402-2000 - IEEE Guide for Electric Power Substation Physical and Electronic Security*, January 30, 2000.
- ⁹⁵ IEEE, January 30, 2000, p. 16.
- ⁹⁶ Institute of Electrical and Electronics Engineers (IEEE), “P1402—Standard for Physical Security of Electric Power Substations,” web page, June 3, 2015, <http://standards.ieee.org/develop/project/1402.html>.
- ⁹⁷ North American Electric Reliability Corporation (NERC), *Threat Alert System and Physical Response Guidelines for the Electricity Sub-sector*, Version 2.0, October 8, 2002, http://www.iwar.org.uk/infocon/threat-levels/tas_physical_V2.pdf.
- ⁹⁸ NERC, October 8, 2002, p. 2.
- ⁹⁹ NERC, October 8, 2002, pp. 3-4.
- ¹⁰⁰ NERC, *Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment*, June 14, 2002, <http://www.esisac.com/Public%20Library/Documents/Security%20Guidelines/Vulnerability%20and%20Risk%20Assessment,%20Version%201.0.pdf>.
- ¹⁰¹ NERC, *Security Guidelines for the Electricity Sector: Physical Response*, November 1, 2005, p.1, <http://www.esisac.com/Public%20Library/Documents/Security%20Guidelines/Physical%20Response,%20Version%203.0.pdf>.
- ¹⁰² NERC, November 1, 2005, p. 3.
- ¹⁰³ FERC Order 706.
- ¹⁰⁴ North American Electric Reliability Corporation (NERC), *NERC: Security Guideline for the Electricity Sub-sector: Physical Security Response*, October 28, 2013, p. 1, [http://www.nerc.com/comm/CIPC/SecurityGuidelinesCurrent/Electricity%20Sector%20Physical%20Security%20Guideline%20\(Approved%20by%20CIPC%20-%20October%2028,%202013\).pdf](http://www.nerc.com/comm/CIPC/SecurityGuidelinesCurrent/Electricity%20Sector%20Physical%20Security%20Guideline%20(Approved%20by%20CIPC%20-%20October%2028,%202013).pdf).
- ¹⁰⁵ NERC, October 28, 2013, p.1.
- ¹⁰⁶ Edison Electric Institute, briefing for the Congressional Research Service, February 23, 2014.

- ¹⁰⁷ Gerry Cauley, CEO, North American Electric Reliability Corporation (NERC), letter to Senator Harry Reid, February 12, 2014, p. 2, <http://www.nerc.com/news/Headlines%20DL/NERC%20Response%20to%20Senators%20Letter%20-Reid%20%202%2011%2014%20v4.pdf>.
- ¹⁰⁸ Federal Energy Regulatory Commission (FERC), *Reliability Standards for Physical Security Measures*, Order Directing Filing of Standards, Docket No. RD14-6-000, March 7, 2014, p.1, <http://www.ferc.gov/CalendarFiles/20140307185442-RD14-6-000.pdf>.
- ¹⁰⁹ FERC, March 7, 2014, p. 2.
- ¹¹⁰ FERC, March 7, 2014, pp. 3-4.
- ¹¹¹ North American Electric Reliability Corporation (NERC), Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard CIP-014-1, May 23, 2014, <http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition%20-%20Physical%20Security%20CIP-014-1.pdf>.
- ¹¹² Federal Energy Regulatory Commission, “Physical Security Reliability Standard,” Docket No. RM14-15-000, Order No. 802, November 20, 2014.
- ¹¹³ North American Electric Reliability Corporation (NERC), *CIP-014-1 – Physical Security*, printed June 4, 2015, p. 1, available at <http://www.nerc.com/pa/Stand/Pages/AllReliabilityStandards.aspx?jurisdiction=UnitedStates>.
- ¹¹⁴ A regional transmission operator (RTO) administers the transmission grid for multiple transmission owners in a specified region in accordance with FERC Order No. 2000. RTOs and independent system operators (ISOs) are defined in Section 3 of the Federal Power Act (16 U.S.C. 796).
- ¹¹⁵ NERC, CIP-014-1, p. 6.
- ¹¹⁶ NERC, CIP-014-1, p. 8.
- ¹¹⁷ Federal Energy Regulatory Commission (FERC), *Statement of Administrative Policy on Processing Reliability Notices of Penalty and Order Revising Statement in Order No. 672*, Docket Nos. AD08-6-000 and RM05-30-002, April 17, 2008.
- ¹¹⁸ Gerry Cauley, President and CEO, North American Electric Reliability Corporation (NERC), Testimony before the House Committee on Energy and Commerce, Subcommittee on Energy and Power, May 19, 2015, p.5.
- ¹¹⁹ For example, see security discussion in Con Edison, “Initial Brief on Behalf of Consolidated Edison Company of New York, Inc. in Support of a Permanent Electric Rate Increase,” Before the New York State Public Service Commission, November 30, 2007, http://media.corporate-ir.net/media_files/irol/61/61493/total120507.pdf.
- ¹²⁰ See Southern California Edison, *Safety, Security, & Compliance (SS&C):Volume 4—Corporate Security and Business Resiliency*, 2015 General Rate Case, Before the Public Utilities Commission of the State of California, November 2013, [http://www3.sce.com/sscc/law/dis/dbattach5e.nsf/0/0B9F998127246B4288257C21008148B0/\\$FILE/SCE-07%20Vol.%2004.pdf](http://www3.sce.com/sscc/law/dis/dbattach5e.nsf/0/0B9F998127246B4288257C21008148B0/$FILE/SCE-07%20Vol.%2004.pdf).
- ¹²¹ Tennessee Valley Authority, “TVA Realigns Security to Enhance Protection at Non-Nuclear Assets,” press release, February 17, 2012, <http://www.tva.gov/news/releases/janmar12/tvap.html>.
- ¹²² “Addressing Cyber and Physical Risks in Modern Utility Security,” *Security*, March 1, 2014, <http://www.securitymagazine.com/articles/85275-addressing-cyber-and-physical-risks-in-modern-utility-security>.
- ¹²³ Rebecca Smith, “U.S. Utilities Tighten Security After 2013 Attack,” *Wall Street Journal*, February 9, 2014.

-
- ¹²⁴ Holly Meyer, “Attacks on Power Grid Point Out Vulnerabilities,” *The Tennessean*, March 24, 2015.
- ¹²⁵ Tennessee Valley Authority, *Budget Proposal and Management Agenda*, February 2015, p. 16.
- ¹²⁶ Tennessee Valley Authority, Form 10-Q, April 30, 2015, p. 57.
- ¹²⁷ Geisha Williams, Executive Vice President of Electric Operations, Pacific Gas and Electric Company, “PG&E Metcalf Attack: Gunfire on Substation Has Led to Greater Security,” *San Jose Mercury News*, April 15, 2014.
- ¹²⁸ “PG&E to Spend \$87M on Security to Protect Large Substations from Attack,” KTVU, Oakland, CA, February 12, 2014.
- ¹²⁹ Pacific Gas and Electric, “PG&E Asks for Public’s Help to Support Theft Investigation at Metcalf Substation,” press release, August 27, 2014.
- ¹³⁰ Dominion. “Substation Security,” fact sheet, Spring 2014, <https://www.dom.com/about/electric-transmission/pdf/substation-security-soc-factsheet.pdf>.
- ¹³¹ Tracy Sears, “Troopers Increase Security at Virginia Substations Critical to Grid,” WTVR, March 11, 2014.
- ¹³² Peter Bacqué, “Va. Power to Spend Up to \$500M on Security Plan,” *Richmond Times-Dispatch*, February 8, 2014.
- ¹³³ David Roop, Director Electric Transmission Operations, Dominion Virginia Power, “Substation Security and Resiliency—Update on Accomplishments Thus Far,” slide presentation, iPCGRID 2015 Conference, March 26, 2015, https://www.cavs.msstate.edu/iPCGRID_Registration/presentations/2015/Roop_iPCGRID_2015_Substation_Security_and_Resiliency.pdf.
- ¹³⁴ Bonneville Power Administration (BPA), *Security Asset Management Strategy*, February 2014, p. 29, <http://www.bpa.gov/Finance/FinancialPublicProcesses/CapitalInvestmentReview/2014CIRDDocuments/Security%20Full%20Asset%20Strategy%20Final%20Draft.pdf>.
- ¹³⁵ BPA, February 2014, p. 31.
- ¹³⁶ BPA, “2nd Quarter Capital Project Status Report,” May 16, 2015, p. 1, <http://www.bpa.gov/Finance/AssetMgmt/CapitalProjectStatusReports/Q2-2015-External-Quarterly-Project-Status-Report.pdf>.
- ¹³⁷ BPA, “500kV Spare Transformer Procurement,” fact sheet, 2015, <http://www.bpa.gov/Finance/AssetMgmt/ProjectSynopsis/500-kV-Spare-Transformer-Project.pdf>.
- ¹³⁸ New York Power Authority, Memorandum to the Trustees Regarding NERC CIP Version 5 Physical and Cyber Security Upgrades—Capital Expenditure Authorization Request and Contract Award, January 27, 2015.
- ¹³⁹ New York Power Authority, Request for Proposals No. Q14-5730RH, September 10, 2014.
- ¹⁴⁰ Corina Rivera Linares, “Pepco’s Capital Expenditure Forecast for 2014-2018 Includes \$157M for Three More Transmission Projects,” TransmissionHub, May 7, 2015.
- ¹⁴¹ William Gausman, Pepco Holdings, “Physical Security Electric Grid,” slide presentation, Mid-Atlantic Conference of Regulatory Utilities Commissioners, June 25, 2014.
- ¹⁴² P.L. 107-56 §1016(e).
- ¹⁴³ North American Electric Reliability Corporation (NERC), “Security Guideline for the Electricity Sector: Identifying Critical Assets,” September 17, 2009, p. 1, http://www.nerc.com/fileUploads/File/Standards/Reference%20Documents/Critical_Asset_Identification_2009Nov19.pdf.
- ¹⁴⁴ FERC, March 7, 2014, p. 3.
- ¹⁴⁵ FERC, March 7, 2014, p. 3.

-
- ¹⁴⁶ FERC, March 7, 2014, p. 3.
- ¹⁴⁷ NERC, CIP-014-1, pp. 24-25.
- ¹⁴⁸ FERC, March 7, 2014, p. 3.
- ¹⁴⁹ NERC, CIP-014-1, p. 22.
- ¹⁵⁰ Foundation for Resilient Societies, Reliability Standard for Physical Security, Request for Rehearing on FERC Order No. 802, Docket No. RM14-15-000, Submitted to FERC on December 21, 2014, p. 8.
Filed by the Foundation for Resilient Societies
- ¹⁵¹ Federal Energy Regulatory Commission (FERC), Order Denying Rehearing, Docket No. RM14-15-001, April 23, 2015, p. 5.
- ¹⁵² FERC, April 23, 2015, p.5.
- ¹⁵³ FERC, April 23, 2015, p.5.
- ¹⁵⁴ For an overview, see Federal Energy Regulatory Commission (FERC), “Critical Energy Infrastructure Information (CEII) Regulations,” web page, June 28, 2010, <http://www.ferc.gov/legal//maj-ord-reg/land-docs/ceii-rule.asp>.
- ¹⁵⁵ Federal Energy Regulatory Commission (FERC), Order No. 630, Final Rule, February 21, 2003, <http://elibrary.ferc.gov/idmws/common/opennat.asp?fileID=9639612>.
- ¹⁵⁶ FERC, March 7, 2014, p. 10.
- ¹⁵⁷ Senate Committee on Energy and Natural Resources, “Sens. Landrieu, Murkowski Ask Inspector General to Examine Leaks of Grid Vulnerabilities,” press release, March 27, 2014; The Honorable Cheryl LaFleur, Chairman (Acting), Federal Energy Regulatory Commission (FERC), Testimony Before the Senate Committee on Energy and Natural Resources Hearing, “Keeping the Lights On—Are We Doing Enough to Ensure the Reliability and Security of the U.S. Electric Grid?,” April 10, 2014.
- ¹⁵⁸ Bobby McMahon, “Wellinghoff Says FERC Analysis of Grid Vulnerability was Public, Calls Review ‘Waste of Time’,” *Inside FERC*, March 31, 2014, p. 1.
- ¹⁵⁹ U.S. Department of Energy, Office of Inspector General, “Review of Internal Controls for Protecting Non-Public Information at the Federal Energy Regulatory Commission,” DOE/IG-0906, April 2014, p. 1.
- ¹⁶⁰ The Honorable Cheryl LaFleur, Testimony on April 10, 2014.
- ¹⁶¹ U.S. Department of Energy, Office of Inspector General, (DOE/IG) “Review of Controls for Protecting Nonpublic Information at the Federal Energy Regulatory Commission,” DOE/IG-0933, January 2015, p. 1.
- ¹⁶² DOE/IG, January 2015, p. 6.
- ¹⁶³ DOE/IG, January 2015, p. 6.
- ¹⁶⁴ See, for example, Michael Wills, “Changes at Duke Energy Substations Crack Down on Copper Thieves,” *WUNC Radio 91.5*, May 22, 2013; Scott Kraus, “Hit Hard by Copper Wire Thieves, PPL Fights Back,” *The Morning Call* (Lehigh, PA), June 6, 2013.
- ¹⁶⁵ Electric Power Research Institute (EPRI), *Technologies for Remote Monitoring of Substation Assets: Physical Security*, March 2006, p. viii.
- ¹⁶⁶ EPRI, September 30, 2104, pp. 24-25 and pp. 37-38.
- ¹⁶⁷ Florida Public Service Commission (FPSC), *Review of Physical Security Protection of Utility Substations and Control Centers*, December 2014, p. 31.
- ¹⁶⁸ Pacific Gas and Electric, “Recommendations for Security,” memorandum, August 30, 2014, p. 1, available at <https://s3.amazonaws.com/s3.documentcloud.org/documents/2081637/pg-amp-e-memo-august-30-2014.pdf>.
- ¹⁶⁹ FPSC, December 2014, p. 25.

-
- ¹⁷⁰ Gerry Cauley, President and CEO, North American Electric Reliability Corporation (NERC), Letter to Senate Majority Leader Harry Reid, February 12, 2014, p. 2, <http://www.nerc.com/news/Headlines%20DL/NERC%20Response%20to%20Senators%20Letter%20-Reid%20%202%2011%2014%20v4.pdf>.
- ¹⁷¹ See, for example, Philip Shenon, "Threats and Responses: Domestic Security," *New York Times*, June 5, 2003, p. A15.
- ¹⁷² EPRI, September 30, 2104, p. 17.
- ¹⁷³ Rebecca Smith, February 5, 2014.
- ¹⁷⁴ Deborah Carpentier, "NERC Gains in Vegetation Management, Cyber and Physical Security, and Reliability Assurance," *Natural Gas & Electricity* (Wiley Periodicals), May 2014, p. 31, <http://www.crowell.com/files/NERCGains-in-Vegetation-Management-Cyber-and-Physical-Security-and-Reliability-Assurance.pdf>.
- ¹⁷⁵ Michael Chertoff, "Building a Resilient Power Grid," *Electric Perspectives*, May/June 2014, p. 35.
- ¹⁷⁶ Edison Electric Institute, briefing for the Congressional Research Service, February 23, 2014.
- ¹⁷⁷ Edison Electric Institute, "The Electric Power Industry's Commitment to Protecting Its Critical Infrastructure," February 2014, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Critical_Infra_Physical_Protection.pdf.
- ¹⁷⁸ Michael Bardee, Director, Office of Electric Reliability, Federal Energy Regulatory Commission, Testimony before the House Committee on Energy and Commerce, Subcommittee on Energy and Power, May 19, 2015, pp. 7-8.
- ¹⁷⁹ Gerry Cauley, May 19, 2015, p. 7.
- ¹⁸⁰ Thomas A. Fanning, Southern Company, Testimony before the House Committee on Energy and Commerce, Subcommittee on Energy and Power, May 19, 2015, p. 1.
- ¹⁸¹ Thomas A. Fanning, May 19, 2105, pp. 14-15.
- ¹⁸² Gerry Cauley, Testimony before the House Committee on Energy and Commerce, Subcommittee on Energy and Power, transcript, May 19, 2015.
- ¹⁸³ Executive Office of the President, *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*, August 2013, p. 12.
- ¹⁸⁴ Mike Kormos, PJM, as quoted in "Physical Security Cure: More Transmission?," *RTO Insider*, July 1, 2014.

INDEX

A

access, x, xi, 4, 19, 29, 32, 39, 40, 41,
47, 59, 64, 71, 74, 77, 78, 91, 92, 96,
98, 100, 118, 122, 129, 132, 136, 137,
142
actuation, 38
actuators, 67
agencies, xii, 21, 34, 48, 52, 55, 60, 81,
82, 83, 84, 86, 98, 103, 107, 109, 110,
122, 123, 130, 131, 133, 136, 138
American Recovery and Reinvestment
Act of 2009, 8, 43
appropriations, viii, 2, 9, 11, 12, 27
Appropriations Act, 10, 11, 12, 13, 79
Appropriations Committee, viii, 2, 11,
12
assessment, 48, 55, 87, 88, 98, 125, 128,
132, 133, 134, 135, 137, 138, 140,
145, 148
assessment models, 137
assets, vii, ix, 3, 7, 13, 18, 20, 24, 26, 32,
38, 44, 46, 51, 67, 77, 78, 81, 87, 88,
89, 94, 99, 102, 103, 104, 105, 121,
122, 130, 131, 134, 138, 143, 144,
146, 147, 153
audit(s), 46, 61, 132, 134
authentication, 72, 78
authority(ies), 34, 43, 44, 45, 46, 47, 48,
49, 61, 65, 71, 76, 95, 96, 98, 99, 102,
128, 132, 134, 136, 141, 143, 146

automation, 47, 70, 75, 106

B

base, 24, 43, 53, 65, 69, 78, 90, 93, 102,
128, 139
batteries, 14, 20, 21
benefits, 26, 49, 140, 142, 148
biomass, 26, 33
blackouts, vii, 3, 17, 29, 42, 112, 116,
117
Bulk Power System, v, 28, 63

C

capital expenditure, 115, 137
certification, 45
challenges, 3, 14, 18, 21, 22, 23, 24, 30,
93, 120, 126, 130
cities, 17, 76, 121
classification, 77, 141
clean energy, 13, 22
Clean Power Plan, viii, 2, 27, 102
climate, 3, 8, 25, 30, 121
Climate Action Plan, viii, 2, 8
CO₂, 57
coal, vii, 2, 16, 33
collaboration, 24, 35, 79, 124
commerce, ix, 31, 33, 50, 76
commercial, 18, 29, 33, 92, 127

- communication, 3, 10, 15, 18, 20, 47, 52, 60, 69, 71, 85, 103
- communication systems, 20, 69
- communication technologies, 18
- communications channel, 123
- community, 81, 82, 90, 97, 122
- competition, 34, 115
- competitiveness, viii, 2, 6
- complexity, 15, 24, 55, 118
- compliance, x, xi, 30, 32, 45, 46, 47, 53, 54, 55, 64, 65, 77, 78, 86, 96, 99, 102, 103, 108, 134, 136, 144
- computer, vii, ix, 2, 17, 19, 29, 31, 35, 43, 58, 68, 69, 71, 74, 75, 78, 82, 94, 100, 101, 129
- computer simulations, 129
- computer systems, 29, 58
- computerization, vii, 3
- computing, 84, 91, 107
- conditioning, 73
- conference, 28, 44
- confidentiality, xiii, 87, 101, 110
- configuration, 37, 92, 115, 121
- conflict, x, 32, 146
- conflict of interest, x, 32
- Congress, xiii, 10, 11, 13, 14, 27, 31, 34, 35, 43, 45, 53, 65, 69, 79, 95, 96, 97, 104, 105, 110, 112, 128, 131, 138, 140, 144, 145, 147, 148
- connectivity, xi, 64, 65, 89, 137
- consensus, 44, 65, 73, 84, 145, 149
- conservation, 18
- Consolidated Appropriations Act, 10, 11, 12, 13
- constituents, 82
- Constitution, 97
- construction, 23, 115, 136, 141
- consumer goods, 5
- consumers, 4, 5, 6, 49, 55, 61, 71, 110, 139
- consumption, 51, 121
- control power flows, ix, 31, 35, 70
- convergence, 5
- cooling, 113, 114, 119, 122
- cooperation, 23, 25, 30, 78, 80, 135
- coordination, xii, 7, 21, 25, 52, 55, 82, 85, 109, 120, 122, 124, 126, 133, 146
- copper, 42, 113, 115, 135, 142
- cost, viii, x, 2, 3, 6, 18, 21, 30, 32, 38, 40, 47, 48, 55, 61, 73, 78, 91, 93, 96, 108, 115, 127, 128, 142, 143, 144, 147
- costs of compliance, 78
- crimes, 43, 107
- crises, vii, 3, 26
- critical infrastructure, vii, ix, x, 3, 32, 35, 39, 43, 44, 48, 49, 51, 53, 55, 56, 57, 58, 63, 65, 71, 72, 73, 76, 78, 79, 80, 81, 82, 84, 86, 89, 92, 93, 95, 96, 98, 99, 122, 124, 132, 135, 136, 138, 140, 145, 146
- customer data, 50, 72
- customers, 3, 19, 20, 33, 34, 36, 39, 40, 43, 49, 50, 58, 60, 83, 93, 106, 111, 113
- cyberattack, ix, xi, 31, 35, 37, 38, 39, 40, 41, 52, 53, 54, 56, 64, 66, 68, 71, 72, 74, 86, 90, 91, 94, 95, 96, 102, 130
- cybersecurity, v, vii, viii, ix, x, xi, 1, 2, 3, 4, 6, 10, 13, 14, 15, 20, 21, 27, 28, 29, 31, 32, 35, 37, 38, 39, 40, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 55, 56, 60, 61, 62, 63, 64, 65, 70, 72, 73, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 99, 100, 102, 103, 104, 105, 106, 107, 108, 122, 124, 132, 136, 140, 150, 151, 157
- cyberspace, vii, 3
- cycles, 27, 42

D

- data collection, vii, 3
- decentralization, 16
- deficiencies, 55
- degradation, 120
- demonstrations, 7
- denial, 40, 101
- Department of Agriculture, 52

Department of Commerce, 52
 Department of Defense, 52, 91, 107
 Department of Energy (DOE), v, vii,
 viii, 1, 2, 4, 5, 6, 7, 8, 9, 10, 11, 13,
 14, 15, 16, 19, 20, 21, 22, 24, 25, 26,
 27, 28, 29, 30, 36, 46, 47, 48, 49, 51,
 52, 57, 60, 61, 79, 80, 84, 85, 88, 100,
 104, 106, 107, 115, 117, 118, 123,
 124, 126, 128, 131, 133, 141, 147,
 149, 150, 151, 152, 153, 156
 Department of Homeland Security
 (DHS), 39, 43, 48, 52, 53, 55, 61, 65,
 80, 82, 85, 93, 95, 98, 99, 122, 123,
 124, 126, 132, 133, 144, 145, 146,
 149, 151, 152
 deployments, 73
 depository institutions, 99
 depth, 83, 146
 destruction, 116, 117, 127, 138
 detection, xi, 64, 72, 82, 89, 95, 104,
 107, 131, 136, 137
 detection system, 82, 131, 137
 detonation, 41
 dialogues, 72
 digital communication, 5, 6
 disaster, 25, 30
 disclosure, 96, 140, 142
 distributed computing, 91, 107
 distribution, x, xi, 3, 6, 7, 13, 18, 19, 23,
 28, 30, 32, 33, 34, 36, 40, 48, 49, 50,
 51, 56, 57, 64, 66, 67, 69, 70, 74, 76,
 77, 82, 83, 87, 90, 96, 99, 106, 107,
 110, 113, 121, 142
 distribution function, 34
 diversification, 5
 diversity, 56
 domestic demand, 115
 draft, 11, 12, 137
 drought, 17, 24

E

earthquakes, 57
 Eastern Europe, 102
 economic growth, viii, 2, 4

ecosystem, 102
 EISA, ix, x, 16, 26, 32, 35, 38, 43, 44,
 45, 49, 50, 52, 61, 69, 83, 98
 electric current, 15, 16, 22, 113
 electric power, vii, viii, ix, x, xi, xii, 1, 2,
 3, 5, 6, 8, 15, 16, 18, 22, 23, 24, 27,
 31, 33, 34, 35, 38, 39, 40, 42, 43, 49,
 57, 63, 65, 69, 71, 76, 77, 78, 79, 83,
 85, 89, 90, 95, 96, 102, 103, 109, 110,
 111, 112, 116, 117, 123, 124, 126,
 131, 135, 138, 142, 146, 147, 148
 electric power flows, vii, 3
 electricity, vii, viii, ix, x, xi, xii, 1, 3, 4,
 6, 15, 20, 21, 23, 24, 27, 30, 32, 33,
 34, 35, 36, 43, 49, 51, 56, 57, 58, 60,
 63, 64, 65, 66, 67, 69, 70, 71, 76, 79,
 80, 85, 86, 90, 91, 98, 99, 103, 105,
 106, 107, 108, 109, 111, 112, 113,
 116, 117, 123, 124, 130, 132, 133,
 138, 139, 142, 149
 electricity delivery, vii
 electromagnetic, 22, 41, 76
 emergency, viii, 1, 4, 16, 21, 23, 25, 30,
 41, 53, 54, 93, 117, 119, 124, 126,
 127, 128, 142, 146
 emergency preparedness, 4, 21, 23
 emergency response, 16, 25
 employees, 74, 84, 121, 122
 encryption, 71, 78
 energy, vii, viii, 1, 2, 3, 4, 5, 6, 7, 8, 13,
 14, 16, 17, 18, 19, 20, 21, 22, 23, 24,
 25, 26, 27, 28, 29, 30, 33, 35, 36, 37,
 40, 42, 48, 54, 56, 57, 58, 60, 61, 65,
 66, 69, 70, 71, 72, 73, 74, 77, 79, 80,
 88, 89, 94, 95, 99, 100, 104, 105, 106,
 107, 123, 126, 129, 140, 148, 153
 Energy and Water Development (E&W),
 viii, 2, 9, 10, 11, 12, 27
 energy density, 21
 energy efficiency, 26, 30, 70
 Energy Independence and Security Act,
 ix, 26, 32, 35, 43, 57, 69, 83, 98
 Energy Policy Act, ix, 31, 34, 43, 57, 76,
 99, 132

Energy Policy Act of 2005, ix, 31, 43, 76, 99, 132
 Energy Reliability, v, viii, 1, 2, 4, 5, 10, 14, 15, 24, 30, 52, 60, 61, 79, 91, 104, 149
 energy security, 4, 21, 123, 148
 energy storage, vii, viii, 1, 2, 17, 21, 56, 107, 148
 energy supply, 24, 30
 enforcement, 44, 45, 133, 134, 135, 136
 engineering, 69, 108, 115, 121
 England, 120, 150
 environment, 21, 67, 73, 75, 142
 environmental protection, 25
 Environmental Protection Agency (EPA), viii, 2, 27, 52, 102
 EPACT, 76, 95
 equipment, xii, 5, 18, 22, 23, 28, 29, 39, 41, 42, 48, 58, 59, 60, 61, 67, 69, 72, 84, 99, 103, 109, 113, 115, 116, 120, 122, 125, 126, 127, 128, 129, 130, 136, 137, 144, 145
 espionage, 75, 84, 102
 executive branch, 82
 Executive Order, 84, 105
 exercises, xii, 21, 25, 87, 109, 112, 120, 122, 129, 130, 138, 143, 148
 expenditures, 55, 92, 94, 115, 137
 expertise, 21, 23, 51, 76, 82, 90, 105, 138
 explosives, 121, 132
 exports, 23
 extreme weather events, 18

F

federal agency, 48
 federal assistance, 147
 federal authorities, 128, 146
 Federal Bureau of Investigation (FBI), 133, 145, 150
 Federal Energy Regulatory Commission (FERC), ix, x, xii, 31, 32, 43, 44, 45, 46, 47, 48, 49, 50, 52, 54, 59, 60, 61, 65, 76, 77, 86, 95, 99, 102, 103, 110,

117, 127, 128, 129, 130, 131, 132, 133, 134, 136, 138, 139, 140, 141, 142, 144, 145, 146, 149, 150, 151, 152, 153, 154, 155, 156, 157
 federal government, vii, 2, 4, 26, 34, 52, 78, 79, 85, 97, 98, 132, 144
 federal law, 34, 55
 financial, xi, 55, 59, 64, 92, 93, 94, 96, 101
 financial system, 55
 flexibility, 3, 8, 13, 16, 20, 144, 148
 fluctuations, 28, 118
 fuel cell, 56, 91, 107
 fuel shortages, viii, 1
 funding, vii, ix, 2, 8, 11, 12, 14, 15, 22, 24, 26, 27, 79, 124, 127, 128, 147
 funds, 16, 26, 43, 52

G

GAO, 39, 45, 59, 60, 99
 global demand, 115, 116
 governments, viii, 2, 4, 23, 25, 48, 55, 81, 82, 98
 grant programs, 24
 grants, 8, 24, 25, 30
 grid services, 7, 20
 grid technology, 79, 148
 grids, x, 18, 28, 63, 72, 107, 120
 growth, viii, 2, 4, 37, 49, 69
 guidance, 17, 29, 51, 72, 84, 98, 130, 132, 133
 guidelines, 38, 45, 76, 84, 124, 131, 132, 138, 142

H

hacking, 71, 100
 harmonization, 43, 49
 hazards, 24, 57, 148
 health, 16, 20, 27, 99, 138
 High-Voltage Transformer Substations, v, 29, 30, 99, 109
 Homeland Security Act, 43, 96, 104

homes, 18, 29, 66, 113
 House, viii, xii, 2, 10, 11, 12, 27, 54, 55,
 62, 97, 102, 103, 104, 107, 110, 112,
 128, 146, 149, 154, 157
 human, 24, 58, 67, 73, 131, 136, 148
 hurricanes, 17, 118
 hydrogen, 91

I

ICS, 73, 74, 81, 82, 99, 101
 identification, ix, 32, 47, 53, 54, 90, 98,
 102
 improvements, 17, 21, 49, 104, 130, 137,
 143
 Independence, ix, 26, 32, 35, 43, 57, 69,
 83, 98
 individuals, 58, 119, 120
 industry(ies), xii, 3, 4, 8, 10, 16, 19, 21,
 23, 24, 32, 34, 38, 46, 48, 49, 51, 52,
 55, 60, 72, 76, 78, 80, 84, 85, 86, 89,
 90, 93, 94, 95, 96, 109, 110, 112, 115,
 116, 117, 118, 121, 122, 123, 124,
 126, 130, 131, 133, 137, 138, 139,
 140, 141, 142, 144, 145, 146, 147,
 148, 149, 150, 151
 information exchange, 90
 information processing, ix, 31, 35, 71
 information sharing, xi, xii, 21, 25, 55,
 64, 79, 81, 82, 85, 86, 96, 98, 109,
 122
 information technology, ix, 19, 26, 31,
 35, 53, 69, 81, 82
 infrastructure, vii, viii, ix, x, 1, 3, 4, 14,
 16, 17, 18, 20, 23, 24, 25, 30, 32, 34,
 35, 36, 37, 38, 39, 42, 43, 44, 48, 49,
 51, 52, 53, 54, 55, 56, 57, 58, 61, 63,
 65, 66, 68, 69, 71, 72, 73, 76, 78, 79,
 80, 81, 82, 83, 84, 85, 86, 89, 92, 93,
 95, 96, 98, 99, 101, 105, 115, 118,
 123, 124, 126, 132, 135, 136, 138,
 140, 142, 145, 146, 151
 institutions, 29, 81, 99
 integration, viii, 1, 2, 6, 13, 16, 19, 20,
 25, 30, 48, 52, 79, 104

integrity, x, 52, 63, 65, 87, 101, 106
 intelligence, 36, 38, 51, 82, 97, 102
 international standards, 71
 interoperability, 18, 43, 44, 45, 48, 50,
 59, 60, 84, 99, 105
 intrusions, vii, x, xi, 3, 20, 39, 48, 49,
 55, 63, 64, 65, 68, 72, 73, 77, 78, 86,
 95
 investments, xi, xii, xiii, 17, 16, 19, 30,
 48, 50, 64, 86, 92, 93, 95, 109, 110,
 115, 135, 136, 143, 148
 issues, viii, xiii, 1, 4, 11, 23, 27, 28, 29,
 35, 43, 47, 48, 49, 50, 51, 52, 60, 69,
 86, 87, 90, 94, 95, 96, 108, 110, 112,
 126, 131, 138
 iteration, 77

L

law enforcement, 133, 135, 136
 legislation, 29, 55, 57, 92, 108, 146, 148
 litigation, 56
 local area networks, 66
 local authorities, 98, 99
 local community, 90
 local government, 25, 48, 55, 82, 98
 logistics, 128

M

machinery, 66
 magnetic field, 29, 103
 malware, xi, 39, 64, 68, 71, 73, 74, 75,
 101, 102
 management, 7, 13, 16, 17, 18, 19, 21,
 28, 50, 53, 56, 81, 84, 85, 88, 94, 106,
 124, 141, 142, 143, 148
 manipulation, 35, 58, 71
 manufacturing, viii, 2, 39, 41, 107, 115,
 116
 marketing, 66, 120
 measurement, 16, 26, 27, 36
 media, 73, 82, 103, 108, 154
 meter, 40, 41, 72, 100, 106, 107

methodology, 131, 139, 140, 150
 Mexico, 34, 44, 60, 105, 116
 microprocessor, ix, 31, 35, 38, 41, 69, 71
 microturbines, 107
 miniaturization, vii, 3
 mission, 4, 20, 21, 26, 43, 48, 57, 76, 79,
 80, 81, 82, 83, 86, 91, 95
 models, vii, 3, 6, 15, 17, 60, 137, 141,
 145
 modernization, viii, ix, 2, 4, 5, 6, 7, 8,
 16, 22, 25, 31, 35, 38, 46, 54, 69, 98,
 102, 148
 modifications, 46, 137
 modules, 73, 74
 motor control, 6

N

national policy, 123
 National Research Council (NRC), 59,
 120, 150, 152
 national security, viii, 1, 14, 20, 48, 51,
 54, 56, 58, 118, 141, 146
 National Security Agency (NSA), x, 63,
 72, 101
 natural disasters, 57, 81, 84, 124, 136
 natural gas, vii, viii, x, 1, 3, 6, 16, 20,
 21, 23, 30, 32, 33, 49, 56, 65, 69, 105
 natural gas pipeline, x, 32, 56
 natural hazards, 57
 networking, vii, 3
 nodes, xii, 19, 109, 111, 125
 North America, ix, xi, xii, 16, 32, 43, 50,
 57, 59, 60, 64, 76, 85, 99, 105, 110,
 123, 130, 133, 144, 149, 150, 151,
 152, 153, 154, 155, 157
 North American Electric Reliability
 Corporation (NERC), ix, xi, xii, 16,
 28, 32, 43, 46, 47, 59, 60, 64, 76, 77,
 85, 86, 94, 99, 102, 103, 105, 108,
 110, 123, 124, 128, 129, 130, 131,
 132, 133, 134, 138, 139, 141, 143,
 144, 146, 149, 151, 152, 153, 154,
 155, 156, 157
 nuclear weapons, 54

O

Obama, President Barack, viii, 2
 Office of Electricity Delivery, v, viii, 1,
 4, 5, 52, 60, 61, 79, 104
 Office of Management and Budget
 (OMB), 12
 officials, 100, 117, 121, 131, 133, 135,
 140, 142, 145, 146
 oil, vii, 3, 20, 21, 29, 49, 69, 113, 114,
 118, 119
 operating system, 19, 75, 100
 operations, ix, xi, 5, 7, 15, 16, 18, 19, 23,
 31, 35, 37, 41, 42, 47, 54, 64, 67, 70,
 73, 74, 75, 86, 89, 91, 95, 97, 106,
 108, 120, 135, 136
 opportunities, 3, 6, 137
 optimization, 7, 18, 19, 28, 70
 oversight, vii, ix, xiii, 11, 32, 46, 47,
 110, 134, 138, 148, 151
 ownership, 94, 128

P

Pacific, 9, 57, 136, 155, 156
 participants, 15, 44, 90, 96, 105, 122,
 124, 130
 penalties, 43, 44, 53, 55
 permit, 48, 52, 61, 98
 perpetrators, 145
 personal communication, 10, 149, 150,
 152
 personal computers, 30
 PES, 57
 petroleum, 6, 23, 65, 105
 pipeline, x, 32, 49, 57, 69
 plants, vii, 2, 15, 16, 27, 33, 34, 36, 38,
 56, 68, 77, 102, 113, 115, 116, 117,
 118, 123
 platform, 6, 7, 14, 18, 19
 police, 120, 135
 policy, 4, 23, 25, 48, 49, 51, 61, 69, 84,
 94, 98, 102, 105, 112, 123, 124, 134,
 144, 147, 148

policy issues, 112
 policymakers, 146
 polymer, 136
 portfolio, 17
 potential benefits, 49
 POWER, 103
 power generation, 3, 15, 16, 21, 27, 33,
 34, 36, 37, 56, 121
 power lines, 18, 66
 power plants, vii, 2, 15, 16, 33, 34, 38,
 56, 68, 117, 123
 power production, vii, 2, 56
 predictability, 22
 preparation, 58, 146
 preparedness, 4, 21, 23, 25, 53, 55, 130
 preservation, 148
 President, viii, 2, 8, 12, 53, 54, 58, 84,
 85, 104, 107, 127, 146, 147, 154, 155,
 157
 prevention, xiii, 82, 98, 110, 146, 148
 private information, 98
 private sector, viii, 2, 23, 25, 52, 81, 82,
 83, 84, 86, 96, 103, 122, 126, 129,
 147
 probability, 94, 142
 process control, 68
 procurement, 72, 87
 producers, 34, 60
 professional development, 79
 project, 14, 61, 84, 91, 108, 125, 137,
 153
 protection, ix, xi, xiii, 7, 25, 32, 43, 44,
 49, 55, 56, 64, 71, 76, 77, 80, 86, 89,
 92, 93, 94, 95, 96, 98, 104, 105, 110,
 125, 131, 136, 140, 147, 151
 prototype, 83, 126
 public awareness, 53
 public health, 99, 138
 public policy, 4
 public safety, 121
 public sector, 93
 public welfare, 51
 public-private partnerships, 82

R

radio, 65, 68, 100
 ratepayers, 50, 143
 real time, 71, 82, 95, 102
 recognition, ix, 31, 43, 44, 69
 recommendations, iv, 11, 12, 45, 84, 94,
 126, 132, 133, 141
 recovery, x, xii, xiii, 17, 22, 30, 32, 41,
 48, 50, 54, 55, 56, 57, 58, 61, 78, 81,
 83, 91, 93, 95, 98, 104, 109, 110, 122,
 124, 125, 127, 130, 136, 146, 147,
 148
 regulations, ix, x, 28, 32, 35, 46, 47, 50,
 53, 65, 77, 129, 141, 142
 regulatory changes, 34
 regulatory requirements, xiii, 110, 148
 reliability, ix, 3, 6, 7, 16, 17, 19, 21, 23,
 24, 25, 27, 30, 31, 34, 35, 36, 40, 41,
 43, 46, 47, 49, 54, 55, 56, 59, 60, 65,
 67, 70, 76, 77, 81, 86, 92, 95, 99, 102,
 106, 111, 120, 123, 124, 125, 126,
 127, 132, 133, 134, 135, 138, 146,
 149, 150, 151
 remediation, 98, 105, 124
 remote sensing, 57
 renewable energy, viii, 1, 2, 13, 21, 25,
 27, 36, 56, 100, 107
 requirements, ix, xiii, 5, 21, 32, 35, 40,
 43, 44, 45, 47, 52, 53, 55, 56, 77, 78,
 84, 92, 96, 98, 106, 110, 115, 120,
 127, 133, 134, 139, 143, 144, 147,
 148
 research and development (R&D), viii,
 2, 4, 6, 10, 13, 14, 15, 16, 17, 18, 21,
 22, 26, 27, 28, 83, 86, 103
 reserves, 126, 128, 147
 resilience, vii, x, xiii, 3, 7, 8, 16, 17, 18,
 21, 22, 63, 65, 72, 79, 81, 83, 90, 98,
 108, 110, 123, 125, 126, 147, 148
 resources, viii, xi, 1, 3, 5, 6, 7, 13, 20,
 21, 23, 28, 34, 35, 36, 41, 48, 49, 52,
 56, 59, 64, 70, 71, 77, 90, 92, 99, 101,
 105, 106, 124, 135, 140, 144

response, viii, 1, 4, 13, 16, 21, 23, 25,
28, 30, 49, 53, 58, 60, 65, 70, 78, 81,
82, 92, 105, 106, 124, 130, 132, 135,
136, 141, 146

restoration, 18, 19, 23, 30, 54, 151

restrictions, 120

restructuring, 115

risk(s), xii, 4, 8, 16, 17, 21, 22, 24, 35,
38, 39, 42, 45, 46, 50, 53, 54, 55, 56,
70, 71, 73, 78, 81, 82, 83, 84, 86, 87,
88, 93, 94, 96, 98, 99, 102, 110, 112,
113, 117, 118, 123, 125, 126, 131,
132, 133, 134, 135, 136, 137, 138,
139, 140, 141, 143, 144, 145, 146,
154

risk assessment, xii, 87, 88, 110, 132,
133, 134, 137, 138, 141, 144

risk management, 56, 81, 84, 88, 93

risk profile, 144

rules, 45, 54, 92, 95

rural areas, 121

S

sabotage, 58, 75, 111, 121, 130

safety, 20, 21, 48, 50, 75, 102, 107, 121,
126, 135, 138

scope, 35, 36, 77, 102, 132, 135, 139

Secretary of Defense, 54

Secretary of Homeland Security, 54

secure communication, 40, 70

security, vii, viii, ix, x, xi, xii, xiii, 1, 3,
4, 14, 18, 20, 21, 29, 32, 38, 39, 40,
43, 44, 45, 46, 47, 48, 50, 51, 53, 54,
56, 58, 60, 61, 63, 64, 65, 68, 70, 71,
72, 76, 77, 78, 79, 80, 81, 82, 83, 84,
85, 86, 87, 88, 89, 93, 94, 95, 98, 99,
100, 101, 102, 103, 104, 105, 107,
108, 109, 110, 112, 113, 117, 120,
121, 122, 123, 124, 125, 126, 129,
130, 131, 132, 133, 134, 135, 136,
137, 138, 139, 140, 141, 142, 143,
144, 145, 146, 148, 154, 155

security events, viii, 1

security guard, 136

security practices, xii, 109, 135

security services, 120

security threats, 46, 99, 105, 124, 125,
133, 144, 148

SED, 128, 152

self-evaluations, 80

self-interest, 20

semiconductor, 40, 41

Senate, viii, 2, 10, 11, 12, 53, 61, 153,
156, 157

sensitivity, 141

sensors, 7, 16, 28, 36, 38, 41, 42, 67, 78

servers, 74, 106

services, 7, 15, 20, 24, 26, 28, 30, 52, 58,
79, 104, 106, 111, 120, 129, 147

signals, 13, 19, 78, 106

simulation, 13, 17, 20, 81, 129, 131

Smart Grid, v, viii, ix, x, xi, 2, 5, 8, 10,
13, 15, 16, 18, 19, 26, 27, 28, 29, 31,
32, 35, 36, 37, 38, 40, 41, 42, 43, 44,
45, 46, 47, 48, 49, 50, 51, 52, 53, 54,
55, 56, 58, 59, 60, 61, 63, 69, 70, 72,
79, 82, 83, 84, 98, 100, 101, 104, 105,
106, 148

Smart Grid technologies, 52, 56

software, ix, xi, 13, 17, 18, 28, 29, 31,
35, 49, 55, 58, 59, 60, 64, 71, 72, 73,
74, 75, 78, 79, 90, 94, 98, 99, 106,
130

solar technologies, vii, 2

solution, 75, 90, 147

specifications, 115, 127, 128

spending, 10, 26, 50, 137, 143, 144

SSA, 21, 123

stability, 15, 20, 21

stakeholders, 7, 23, 24, 80, 81, 82, 86,
93, 139, 146, 147

state, viii, x, 2, 4, 7, 20, 21, 23, 24, 25,
29, 30, 32, 34, 35, 45, 48, 50, 51, 55,
60, 65, 66, 69, 75, 81, 82, 83, 89, 92,
93, 95, 97, 98, 99, 102, 103, 111, 116,
126, 127, 128, 129, 132, 133, 136,
137, 139, 142, 143, 147, 148

state of emergency, 127

state regulators, 128

statutory authority, 49
 steel, 113, 119
 storage, vii, viii, 1, 2, 3, 6, 17, 21, 23,
 29, 30, 37, 56, 73, 106, 107, 128, 136,
 148
 storage media, 73
 structure, 4, 15, 16, 29, 123, 135, 143,
 147
 suppliers, 51, 72, 74, 106
 supply chain, 17, 72, 84
 supply disruption, 30
 surveillance, 118, 133, 135, 137
 susceptibility, ix, 31, 35, 71
 sustainability, 107

T

target, x, 13, 29, 32, 58, 59, 73, 75, 100,
 120
 Task Force, 52, 61, 114, 149
 technical assistance, 7, 24, 25, 148
 techniques, 18, 19, 52, 83, 130
 technologies, vii, viii, x, xi, 1, 2, 3, 4, 5,
 6, 8, 13, 14, 18, 19, 20, 21, 22, 26, 28,
 31, 35, 36, 44, 49, 52, 53, 56, 63, 65,
 69, 70, 79, 81, 82, 83, 84, 90, 91, 103,
 104, 106, 107, 108, 120, 124, 135,
 136, 142, 148
 telecommunications, x, 32, 42, 56, 61
 Tennessee Valley Authority, 39, 116,
 135, 154, 155
 territorial, 81
 territory, 105
 terrorism, 80, 98, 127, 144
 terrorist attack, xii, 81, 98, 110, 127,
 142, 145, 146
 terrorists, 35, 84, 120, 140
 testing, 22, 25, 41, 45, 87, 104, 115
 threats, x, xi, xii, 8, 14, 20, 22, 24, 29,
 32, 38, 40, 46, 48, 49, 51, 53, 54, 55,
 63, 64, 65, 76, 80, 82, 83, 85, 86, 89,
 90, 95, 99, 101, 102, 105, 110, 118,
 124, 125, 132, 133, 136, 144, 145,
 148
 Title I, 104

Title II, 104
 trade, 51, 57, 86, 125, 126
 training, 25, 26, 81, 87, 120, 124
 transactions, 16, 36
 transformation, viii, 1
 transmission, xi, xii, 3, 6, 7, 8, 16, 18,
 22, 23, 26, 27, 28, 30, 33, 34, 36, 39,
 50, 56, 58, 59, 60, 66, 67, 69, 76, 77,
 87, 99, 102, 106, 107, 109, 110, 112,
 113, 114, 115, 116, 117, 118, 119,
 120, 127, 129, 130, 132, 133, 134,
 135, 136, 137, 138, 142, 145, 148,
 149, 152, 154, 155
 transport, 22, 58, 127
 transportation, 55, 65, 95, 107, 115, 119,
 147
 treatment, 55, 140
 TVA, 39, 135, 154

U

U.S. economy, x, 63, 64
 U.S. Power Grid, v, 29, 30, 99, 109, 149
 ultimate user, 66
 United Kingdom, 120
 United States (USA), ix, x, xii, 31, 33,
 34, 35, 37, 39, 42, 44, 48, 50, 53, 54,
 57, 60, 63, 64, 69, 80, 81, 83, 98, 102,
 110, 111, 112, 114, 115, 116, 117,
 119, 120, 135, 138, 139, 145, 151
 urban, 16, 113, 151
 USA PATRIOT Act, 138
 utility costs, x, 32, 50

V

validation, 138, 141
 vandalism, 130, 132, 142
 vehicles, 6, 18, 51, 106, 132
 viruses, 58, 71, 94
 vision, 6, 36, 136
 visualization, 8, 14
 vulnerability, xi, 22, 35, 37, 38, 39, 40,
 41, 47, 64, 65, 71, 72, 75, 82, 83, 91,

95, 98, 102, 117, 119, 121, 124, 131,
132, 134, 138, 141, 143, 145, 148

W

Washington, 52, 59, 104
water, x, 3, 30, 32, 56, 58, 63, 65, 72, 95

web, 27, 40, 57, 128, 150, 151, 152, 153,
156
White House, 55, 62, 103
wholesale, 34, 49, 50, 57, 76, 106
wildfires, viii, 1, 17
wind turbines, 33, 107
wireless networks, 40
workforce, 26, 132