Energy Security Initiative
at BROOKINGS





SOFTWARE AND HARD TARGETS:

ENHANCING SMART GRID CYBER SECURITY IN THE AGE OF INFORMATION WARFARE

Charles Ebinger
Kevin Massy

FEBRUARY 2011
Policy Brief 11-01

Energy Security Initiative
at BROOKINGS

SOFTWARE AND HARD TARGETS:

ENHANCING SMART GRID CYBER SECURITY IN THE AGE OF INFORMATION WARFARE

Charles Ebinger
Kevin Massy

FEBRUARY 2011
Policy Brief 11-01

About The Brookings Energy Security Initiative

The Energy Security Initiative (ESI) is a cross-program effort by the Brookings Institution designed to foster multidisciplinary research and dialogue on all aspects of energy security today. ESI recognizes that public and private choices related to energy production and use will shape the global economic, environmental and strategic landscape in profound ways and that achieving a more secure future will therefore require a determined effort to understand the likely consequences of these choices and their implications for sound policymaking. The ESI Policy Brief Series is intended to showcase serious and focused scholarship on topical issues in one or more of these broad research areas, with an emphasis on targeted policy recommendations.

Contact for the Energy Security Initiative:

Govinda Avasarala
Research Assistant
(202) 797-6231
gavasarala@brookings.edu

The authors would like to thank Caldwell Bailey of the Johns Hopkins School of Advanced International Studies and Josh Cornfeld for their research support in the compilation of this report. Thanks also to Dr. Peter Fox-Penner at the Brattle Group for his external review of the manuscript and to the National Association of Regulatory Utility Commissioners for its assistance in distributing the research survey.

The Authors

Charles K. Ebinger

Dr. Charles Ebinger is senior fellow and director of the Brookings Energy Security Initiative. He has more than 35 years of experience specializing in international and domestic energy markets and the geopolitics of energy, with a particular focus on the Middle East, South Asia, Africa, the Arctic and Antarctic. He has served as an energy policy advisor to over 50 governments on restructuring their state-owned energy sectors, privatization and the creation of regulatory regimes. He is an adjunct professor of electricity economics at Johns Hopkins Nitze School.

Kevin Massy

Kevin Massy is the assistant director of the Energy Security Initiative at The Brookings Institution where his research focuses on power markets, nuclear energy, and international energy relations. A former journalist, most recently for *The Economist* magazine, he has written extensively on the role of emerging technologies in the energy sector.

Table of Contents

Introduction

As the United States begins to address the reality of its aging infrastructure and the long-term challenges posed by fossil fuel use, there is widespread recognition that an overhaul of the electric power grid is necessary. Through implementation of the Smart Grid, a system combining information technology and new sources of power generation, the United States has the potential to meet its economic, environmental, and strategic goals while accommodating a projected rise electricity demand. The benefits of the Smart Grid include increased power-system efficiency and reliability; the ability to harness distributed generation; increased integration of renewable energy sources into the energy mix; improved opportunities for energy storage; and increased consumer control of electricity consumption.

However, with the new opportunities come new risks and challenges. The growth of the Smart Grid will create a range of new challenges from the logistical implications of upgrading and replacing large parts of the nation's power infrastructure to devising new business models that balance more efficient delivery of electricity with equity considerations that protect the interests of the economically vulnerable. One of the most important considerations regarding the implementation of the Smart Grid is the new security concerns it raises, particularly in the critical—and rapidly developing—arena of cyber security.

This paper examines the emerging field of Smart Grid cyber security and recommends federal policies that can be enacted to help protect the United States from cyber attacks through the Smart Grid. Parts 1 and 2 provide an overview of the Smart Grid, including its origins, scope, and policy objectives; and the challenge of securing the Smart Grid against cyber vulnerabilities. Part 3 looks at the policies that have been implemented at the federal, state, and local levels to do so, and is informed by responses of several U.S. State Public Utility Commissions to a Brookings-designed survey (see Appendix II). The report concludes by offering a series of recommendations for more effective policymaking in the arena of Smart Grid cyber security.

Smart Grid

Definition of the Smart Grid

The Smart Grid aims to combine the benefits of information technology with new and existing energy generation and storage technologies to deliver a more efficient, flexible power infrastructure. According to the Department of Energy's (DOE) National Energy Technology Lab, "the Smart Grid isn't a thing, but rather a vision."[1] A more comprehensive definition, provided by Peter Fox-Penner in his book *Smart Power*, describes the Smart Grid as a system that combines "time-based prices with the technologies that can be set by users to automatically control their use and self-production, lowering their power costs and offering other benefits to the system as a whole."[2]

While many of the concepts underpinning the Smart Grid have been understood for decades, the origins of the Smart Grid as an integrated whole was articulated most fully by Congress in the 2007 Energy Independence and Security Act (EISA), which defined the Smart Grid as comprising the following:

1. Increased use of digital information and controls technology to improve reliability, security and efficiency of the electric grid.
2. Dynamic optimization of grid operations and resources, with full cyber security.
3. Deployment and integration of distributed resources and generation, including renewable resources.
4. Development and incorporation of demand response, demand-side resources and energy-efficiency resources.
5. 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.
6. Integration of "smart" appliances and consumer devices.
7. Deployment and integration of advanced electricity storage and peak-sharing technologies, including plug-in electric and hybrid electric vehicles, and thermal-storage air conditioning.

[1] National Energy Technology Laboratory, *The Modern Grid Strategy: A Vision for the Smart Grid*, National Energy Technology Laboratory, June 2009, 5.
[2] Fox-Penner, Peter, *Smart Power: Climate Change, The Smart Grid, and the Future of Electric Utilities* (Island Press, 2010), 47.

8. Provision to consumers of timely information and control options.

9. Development of standards for communication and interoperability of appliances and equipment connected to the electric grid, including the infrastructure serving the grid.

10. Identification and lowering of unreasonable or unnecessary barriers to adoption of Smart Grid technologies, practices and services.

Policy Drivers and Benefits of the Smart Grid

According to the U.S. DOE, the policy motivations for the Smart Grid are: increased efficiency, increased reliability, long-term affordability for customers, increased security, decreased environmental impact, and an increased potential for economic innovation. The smart grid allows these objectives to be met through three principal means:

Dynamic pricing: an approach to differentiating electricity pricing according to demand patterns, thereby creating a more competitive market for retail electricity. The Smart Grid enables dynamic pricing through two-way communication that allows consumers to respond to changes in electricity prices. This, in turn, enables grid operators to "balance" the grid by shifting the demand—as well as the supply—for electricity. The benefits of dynamic pricing are enormous. A 2008-2010 study conducted by PEPCO, a utility serving Maryland and Washington, D.C., found that differentiated pricing plans could result in reductions of peak load by as much as 34 percent.[3] If such outcomes are realizable at scale, dynamic pricing has the potential to reduce the number of back-up power plants needed to provide power at times of peak demand, leading to reduced costs for customers (who do not have to pay for additional construction) and increased system efficiency. Shifting loads can also create large reliability benefits as grid operators can incentivize consumers to reduce their electricity use during periods of system stress in order to prevent power outages. The integration of dynamic pricing depends on the widespread adoption of Smart Metering technologies, which allow consumers to automate their consumption of electricity in relation to the real-time price of kilowatt hours.

Distributed generation: the use of small, local and, in many cases, renewable energy resources to the electricity grid. The Smart Grid will simplify the interconnection regime for distributed generation resources and will create an interoperability framework enabling a range of power generators to more easily connect to the grid. When combined with "net metering" policies by utilities, which let customers sell electricity back into the grid at the same price as they buy it, distributed generation has the potential to accelerate the adoption of small-scale renewable energy, thereby reducing the carbon intensity of the electric grid.

Energy storage: the use of batteries, electric cars, and other technologies to provide electricity to the power grid in times of stress and high prices. The Smart Grid will create a system that notifies owners of energy storage devices when prices are high so they can sell their excess electricity back to the grid, lessening the stress on centralized sources of generation and reducing the risk of power outages. In combination with dynamic pricing structures, owners of energy storage technologies will also be able to buy electricity when prices are low, thus "flattening the load curve" and increasing the efficiency of the power grid through reduced reliance on low-efficiency power plants.

[3] PEPCO, *PowerCentsDC Program, Final Report*. PEPCO, September 2010, 3.

The Smart Grid also has further reliability and security benefits. It allows grid operators to respond more rapidly to power outages and other disturbances. Through the integration of sensors and two-way communication into the power system, electric utilities can detect—and respond to—outages as they occur. The same remote diagnostic capability allows operators to recognize when the grid has been the subject of attack. The constant flow of information from the electric grid will help stabilize power quality, which is increasingly important as the United States moves further into the digital economy

Smart Grid Deployment

In the 2007 Energy Independence and Security Act (EISA), Congress required DOE to prepare a Smart Grid Systems Report for the purpose of briefing Congress on the status of Smart Grid deployment across the country. In 2009, the DOE published the first Smart Grid Systems Report. The report identified twenty metrics for measuring the status of Smart Grid deployment and impacts. The metrics are characterized as either "build" or "value" metrics. According to DOE, "Build metrics describe attributes that are built in support of a Smart Grid, while value metrics describe the value that may derive from achieving a Smart Grid."[4] The DOE organized a workshop with representatives from the electric utility industry to determine the penetration level (for build metrics) or maturity level (for value metrics), and the trending direction of each metric. The results from the workshop were presented in the report and are reproduced in Appendix I.

[4] United States Department of Energy, *Smart Grid System Repo*rt, United States Department of Energy, June 2009, v.

Smart Grid Security

The Smart Grid has the potential to bring economic, reliability and environmental benefits to America's electric utility industry. However, the implementation of Smart Grid will also present a range of new security and reliability concerns, particularly in the cyber security arena.

Defining Smart Grid Security

Security of the Smart Grid can be divided into three categories: physical security, data security and cyber security. Physical security relates to protection of the Smart Grid's physical infrastructure including advanced meter interface (AMI) hardware, such as smart meters, transmission lines, generating equipment and control rooms from damage. Such damage can be the result of intentional attacks using electromagnetic pulses or other weapons, or unintentional as the result of damage from electric storms. Data security refers to the privacy of the information that is transferred over the Smart Grid; it relates to customer information such as personal details, financial information and energy-usage patterns that can be misappropriated by hackers to do damage to individuals. Cyber security relates to the vulnerability of the grid to intentional infiltration by hackers using the Internet or other digital-information management systems with the intention of disrupting the normal operation of the power delivery system.

Smart Grid Security Objectives

From the inception of the Smart Grid concept, security has been recognized as a primary policy objective. The first two Smart Grid-related provisions of the 2007 EISA emphasized the "reliability, *security* and efficiency of the electric grid"[5] and the "dynamic optimization of grid operations and resources, *with full cyber security,*"[6] respectively. The Obama administration has also recognized the importance of Smart Grid security. In its 2009 Cyberspace Policy Review, the White House underlined the need for the federal government to "ensure that security standards are developed and adopted to avoid creating unexpected opportunities for adversaries to penetrate these systems or conduct large-scale attacks"[7] in the deployment of the Smart Grid. Numerous federal agencies have issued warnings about the need for Smart Grid security. In its National Infrastructure Protection Plan, the Department of Homeland Security (DHS) ac-

[5] Energy Independence and Security Act of 2007 (EISA), *Title XIII*, EISA, 2007, 2.
[6] Ibid., 2.
[7] Testimony before the House Committee on Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, United States House of Representatives (July 21, 2009, 4) (Testimony of Cita M. Furlani, Director, Information Technology Laboratory).

knowledged that the cyber security vulnerabilities in the IT and telecommunications systems would also have to be assessed in the context of the Smart Grid. Moreover, DHS recognized that the Smart Grid would have additional vulnerabilities "due to its complexity, large number of stakeholders, and highly time-sensitive operational requirements."[8] The Federal Energy Regulatory Commission (FERC) has also identified cyber security as "essential to the operation of the Smart Grid."[9] In its 2009 Smart Grid Policy Statement, FERC stated that it regarded development of cyber security standards as "a key priority" and that it believed that "implementation of smart grid technology, which is designed to improve communication, coordination, and interoperability, will require added attention to cybersecurity standards."[10] As part of its focus on Smart Grid security, FERC has called for compliance with the National American Electric Reliability Corporation (NERC)'s eight critical infrastructure protection (CIP) standards. These eight standards (outlined below) constitute NERC's primary recommendations for enhancement of cyber security of the bulk power system.

The National Institute of Standards and Technology (NIST), which was given a mandate under the EISA to coordinate Smart Grid interoperability standards, has also highlighted the security concerns associated with adoption of the Smart Grid. In its Smart Grid Cyber Security Strategy, NIST warned that the implementation of the Smart Grid would lead to an increase in the importance of information technology and communications infrastructure in the power system. In NIST's view, "the security of systems and information in the IT and telecommunications infrastructures must be addressed by an evolving electric sector."[11]

The Cyber Security Threat

As early as 1997, a Presidential Commission on Critical Infrastructure Protection highlighted cyber attacks as points of vulnerability owing to the increased reliance of the nation's power infrastructure on supervisory control and data acquisition (SCADA) systems.[12] A 2003 report from the Government Accountability Office (GAO) echoed the concern with the cyber vulnerability of the power grid and suggested several steps to address the threats, including the development of new technologies to protect control systems, the development of security policies and standards, and the increased sharing of information about security architectures.[13] While the SCADA systems that control the electrical infrastructure are notionally separate from each other, the Internet provides a determined saboteur with an access channel, often through the portal of corporate intranets.[14] The GAO found "a number of factors, including the interconnectivity of [SCADA] systems, their connection to the Internet, non-secure connections, and the availability of pertinent technical information, that make supervisory control and data acquisition systems susceptible to cyber threats and vulnerabilities."[15]

---

[8] NIST Office of the National Coordinator for Smart Grid Interoperability, *NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft)*, NIST Office of the National Coordinator for Smart Grid Interoperability, September 2009, 75.

[9] Federal Energy Regulatory Commission, *18 CFR Chapter [Docket No. PL09-4-000] Smart Grid Policy*, Federal Energy Regulatory Commission (July 16, 2009, 19).

[10] Ibid., 19.

[11] NIST, The Smart Grid Interoperability Panel – Cyber Security Working Group. *Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements*, NIST, The Smart Grid Interoperability Panel – Cyber Security Working Group, August 2010, 1.

[12] The Report of the President's Commission on Critical Infrastructure Protection, *Critical Foundations Protecting America's Infrastructures*, (October 1997).

[13] Testimony before the House Committee on Government Reform, (October 1, 2003) (Testimony of Robert F. Dacey, Chief Accountant for the United States Government Accountability Office-GAO).

[14] Clarke, Richard A, *Cyber War: The Next Threat to National Security and What to Do About It* (Ecco, April 2010), 99.

[15] The Government Accountability Office, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, (2007).

Once a SCADA system has been compromised by a cyber attack, hackers can harm the electric grid by causing power outages or even destroying generating equipment. In 2007, CIA Analyst Tom Donahue caused consternation within the national security community when he revealed that cyber attacks had caused power outages in many different countries worldwide. During the Russian-Georgian war in 2008, cyber attacks widely believed to have originated in Russia, brought down the Georgian electric grid during the Russian Army's advance through the country.[16] In April 2009, the *Wall Street Journal*, quoting current and former national security officials, reported that "cyberspies" had penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system.[17] Moreover, cyber attacks have been shown to have the capability to destroy generating equipment. In March 2007, DOE's Idaho National Laboratory conducted an experiment known as the "Aurora Generator Test," in which physical damage was caused to a diesel generator through exploitation of a security flaw in its SCADA system.[18] The so-called "Aurora Vulnerability" is still a security concern today.

Cyber security and the Smart Grid

Even as these well-documented cyber security vulnerabilities in the legacy electric grid continue to exist, the growth of the Smart Grid is creating new cyber security concerns. Two-way communication has the potential to create a new avenue for cyber attacks to reach the bulk power system and cause serious damage to this critical infrastructure by way of a customer's smart meters and other grid-connected smart technology. In his testimony before Congress in July 2009, FERC Director of the Office of Electric Reliability Joseph McClelland said, "A smarter grid would permit two-way communication between the electric system and a large number of devices located outside of controlled utility environments, which will introduce many potential access points."[19] McClelland said an attacker who gained access to the communication channels could order metering devices to disconnect customers, order previously shed load to come back on line prematurely, or order dispersed generation sources to turn off during periods when load is approaching generation capacity, causing instability and outages on the bulk power system.[20] The recognition of the cyber security vulnerabilities of the Smart Grid are shared by utilities. In testimony before Congress, Sacramento Municipal Utility District General Manager and CEO John DiStasio said Smart Grid applications provided "new vectors for attack" on new and existing utility systems."[21] The applications of most concern with regard to Smart Grid cyber security are smart meters and new sources of distributed generation and storage.

Smart meters: Around 60 million smart meters are expected to be deployed across the United States by 2019.[22] While these devices will give customers unprecedented access to information and control over their electricity usage, they will also provide a large new target for would-be saboteurs. According to cyber security analysts, smart

[16] Markoff, John, "Georgia Takes a Beating in the Cyberwar with Russia," *The New York Times,* August 11, 2008.
[17] Gorman, Siobhan, "Electricity Grid in U.S. Penetrated by Spies," *The Wall Street Journal,* April 8, 2009.
[18] PriceWaterhouseCooper, *Cyber attacks: Is your critical infrastructure safe?,* PriceWaterhouseCooper, 2010.
[19] Testimony before the House Committee on Homeland Security (July 21, 2009, 6) (Statement of Joseph McClelland, Director, Office of Electric Reliability, Federal Energy Regulatory Commission).
[20] Ibid., 6-7.
[21] Statement to the House Subcommittee on Energy and Environment, *Protecting the Electric Grid: H.R. 2165, the Bulk Power System Protection Act of 2009, and H.R. 2195*, (October 27, 2009) (Statement by John DiStasio, General Manager and CEO of the Sacramento Municipal Utility District-SMUD).
[22] Owens, David K., Edison Electric Institute, "National Electricity Market Update: An Industry Overview," Paper presented by Edison Electric Institute at the 27th Annual EEI Supplier Diversity Conference, May 18, 2010.

meters may be used by hackers as entry points into the broader power system.[23] In March 2010, InGuardians, a security consulting firm hired by three electric utilities, found serious vulnerabilities in ZigBee, the low-power communications wireless protocol used to link devices to smart meters through home area networks. InGuardians found that it could hack into the communications stream between a customer and a utility company, providing a potential channel for an attack on the grid. The study followed a similar finding from IOActive, a security services firm, that hackers could hack into smart meters to "take command and control of the [advanced metering infrastructure], allowing for the en masse manipulation of service to homes and businesses."[24] The infiltration of smart meters is particularly concerning as many devices can be compromised through a single software vulnerability. The prospect of a proliferation of vendors selling AMI hardware and software with little or no compatibility multiplies the threat. In August 2010, market research firm Pike Research released a report addressing the vulnerability of smart meters. According to Bob Lockhart, an industry analyst quoted in the report, "Smart meters are one of the weakest links in the smart grid security chain."[25] The report found that, while home area networks, commercial building networks and utility networks all perform well in terms of keeping data encrypted within their domains, these domains terminate at the smart meter.

Distributed Generation and storage: Distributed Generation (DG) technologies include rooftop solar installations, "microwind" turbines, electrochemical fuel-cell systems, and combined heat and power applications. Distributed energy storage includes advanced batteries and vehicle-to-grid (V2G) systems, through which cars are used to store off peak electricity and to supply it back to the grid when demand is high. By using localized sources of distributed generation and storage, electricity consumers in the commercial and residential sectors have an opportunity to bypass the centralized system of generation and dispatch to meet their own electricity needs, to profit from net metering arrangements with utilities, and to provide a source of increased stability to the bulk power system. While these attributes are undoubtedly positive, the opening of the grid to many thousands of new access points raises the same concerns as those associated with the proliferation of smart meters above. A further consideration, with regard to distributed generation and storage, is the prospect of increased reliance by grid operators on them for balancing and system stability. As DG resources become a large part of the electricity supply mix, they become far more than the sum of their parts. In testimony before Congress, NERC Vice President and Chief Security Council Michael Assante stated that while a single device would not be considered material to bulk power system reliability, "in aggregate, these assets may become critical to the bulk power system."[26] Considerations such as these increase the system-wide implications of a DG-based cyber attack. They also have jurisdictional ramifications. While the bulk power system is regulated at federal level (see page 13), distributed resources are not.

---

[23] Mills, Elinor, "Money trumps security in smart-meter rollouts, experts say," CNET News, June 15 2010, accessed on December 28, 2010, <http://news.cnet.com/8301-27080_3-20007672-245.html>.

[24] Testimony before the House Committee on Science and Technology, (July 1, 2010) (Testimony by Lillie Coney, Associate Director, Electronic Privacy Information Center-EPIC).

[25] Pike Research, *Smart Grid Cyber Security*, Pike Research, 2010. Quoted in Pike Research press release, accessed on January 28, 2011 at <http://www.pikeresearch.com/newsroom/smart-meter-security-investment-to-total-575-million-by-2015-but-meters-remain-a-point-of-vulnerability-in-the-smart-grid>.

[26] Testimony before the Committee on Homeland Security, (July 21, 2009, 3) (Testimony by Michael J. Assante, Vice President and Chief Security Officer, North American Reliability Corporation), accessed on December 28, 2010, <http://homeland.house.gov/SiteDocuments/20090721141526-32619.pdf>.

Current Policies and Regulations

Federal Agency Action

Securing the electric grid in order to ensure the reliable delivery of electricity is a priority of the U.S. Government. In the EISA, Congress required DOE to "submit a report to Congress that provides a quantitative assessment and determination of the existing and potential impacts of the deployment of Smart Grid systems on improving the security of the Nation's electricity infrastructure and operating capability."[27] In April 2009, DOE released its *Study of Security Attributes of Smart Grid Systems.* The report found "The implementation of the Smart Grid will include the deployment of many new technologies…. These new technologies will require the addition of multiple communication mechanisms and communication infrastructures that must be coordinated with numerous legacy systems and technologies that are currently installed. These technologies are now in the process of deployment and recent studies have shown that the deployed Smart Grid components have significant cyber vulnerabilities."[28]

The actual securing of the electric grid consists of two parts: 1) federal and state legislation to set grid security policy and 2) the development of standards by technical bodies and non-governmental organizations to secure the electric infrastructure.

The history of grid security legislation starts with the passing of the Federal Water Power Act (FWPA) in 1920. The FWPA created the Federal Power Commission (FPC) to coordinate the development of hydroelectric power plants. The FWPA was amended by the Federal Power Act (FPA) of 1935 to grant the FPC the authority to regulate the sale and transport of electricity across interstate boundaries. In 1977, Congress reorganized the FPC as the Federal Energy Regulatory Commission (FERC) which is in charge of regulating the interstate commerce of electricity today. For Smart Grid security, the most important part of the Federal Power Act is the limitation of FERC's authority to the bulk power system, which Congress defined as:

> "(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and

[27] Energy Independence and Security Act of 2007 (EISA): Timelines, 2, accessed on December 28, 2010, <http://www.eei.org/whatwedo/PublicPolicyAdvocacy/FedLegislation/Documents/TitleXIII.pdf>.

[28] Department of Energy Office of Electricity Delivery and Energy Reliability, *Study of Security Attributes of Smart Grid Systems—Current Cyber Security Issues*, (April 2009, v).

(B) electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy."

With the gradual move to a Smart Grid infrastructure, the bulk power system has the potential to become more vulnerable to cyber attack. According to the House Committee on Science and Technology, "The centralized control systems that manage and control the generation, transmission, and distribution of electric power raise significant cyber security concerns."[29]

Congress reformed grid security regulation through the Energy Policy Act of 2005, which authorized FERC to license an "Electric Reliability Organization" to "establish and enforce reliability standards for the bulk power system." FERC selected the North American Electric Reliability Council (NERC) as the Electric Reliability Organization, tasked with developing the reliability standards, which included standards for "cybersecurity protection." The resulting reliability standards are subject to review by FERC, but FERC is only allowed to approve or reject the standards. FERC does not have the authority to offer amendments.

Standards

To date, NERC has developed eight critical infrastructure protection reliability standards for the cyber security of the bulk power system (CIP 002-009). According to NERC, "NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. The eight standards are:

CIP-002	Critical Cyber Asset Identification
CIP-003	Security Management Controls
CIP-004	Personnel & Training
CIP-005	Electric Security Perimeter(s)
CIP-006	Physical Security of Critical Cyber Assets
CIP-007	Systems Security Management
CIP-008	Incident Reporting and Response Planning
CIP-009	Recovery Plans for Critical Cyber Assets

CIP 002-009 were approved by FERC in 2008. FERC has stated that all companies controlling electric infrastructure in the bulk power system must adopt these standards by the end of 2010 or FERC will begin fining companies $1 million per day until they are adopted.

Congress first considered the effect that the Smart Grid would have on grid security in the Energy Independence and Security Act of 2007. In Section 1305, Congress directed NIST to "coordinate the development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems." FERC stated that all companies controlling electric infrastructure in the bulk power system had to adopt these standards by the end of 2010 or face financial penalties. However, recent research by DOE has shown the existing CIPs and the manner of their implementation by FERC to be unsatisfactory. A January 2011 report by DOE's Office of Audits and Inspections found that the standards "did not always include controls commonly recommended for protecting critical information systems," and that its implementation approach and schedule were not adequate to ensure timely risk mitigation to the power system. One of the principal reasons stated by FERC for the CIP's shortcomings was the commission's lack

[29] 111th session of The United States Congress, Committee on Science and Technology Hearing, *Smart Grid Architecture and Standards: Assessing Coordination and Progress* (July 1, 2010).

of authority to propose remand or direct changes to reliability standards.[30]

NIST is working with stakeholders to develop the Smart Grid Interoperability Framework and has developed 18 Priority Action Plans that will guide formulation of standards to address the gaps in Smart Grid cyber security.[31] According to NIST, there is a three-phase plan for the implementation of Smart Grid standards. Phase one involves the identification of a set of consensus standards and the development of a "roadmap" to fill in the gaps. This was achieved with the release of the *Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0* in January 2010, which included a survey of Smart Grid standards and identified gaps in the overall architecture. Phase two involves the establishment of a Smart Grid Interoperability Panel (SGIP) to provide input to the roadmap and new standards. In August 2010, the Cyber Security Working Group, a sub-committee within SGIP, issued *Guidelines for Smart Grid Cyber Security*, a follow-on document to the Framework. This three-volume document covers high-level risk assessment and mitigation strategies for the Smart Grid, as well as personal privacy and information protection recommendations for individual consumers. The third and final phase of the NIST plan is the development of testing and certification frameworks.

In parallel, and in cooperation with SGIP, DOE has formed the Gridwise Architecture Council (GWAC), based at its Pacific Northwest National Laboratory in Richland, Washington. Since its creation, GWAC has formulated a framework for Smart Grid interoperability across all levels of the Smart Grid supply chain. The framework addresses policy and technical hurdles to interoperability, as well as ways to manage those impediments. The framework also addresses common areas of concern, including Smart Grid system reliability.[32] The GWAC Interoperability Constitution seeks to lay out fundamental aspects of an elegant Smart Grid design, and define business, usability, information technology, regulatory and governance principles that should guide its organization and deployment.[33]

In order to implement these standards, Congress authorized FERC to "institute a rulemaking proceeding to adopt such standards and protocols as may be necessary to insure Smart Grid functionality and interoperability in interstate transmission of electric power, and regional and wholesale electricity markets."[34]

Congressional Action

Widespread concern about the status of grid security in the United States, triggered by reports such as the April 2009 *Wall Street Journal* article on the penetration of the electric grid by Russian and Chinese "cyberspies," caused Congress to begin reconsidering grid security legislation in 2009. Hearings were held in the House Homeland Security, and Energy and Commerce Committees, and the Senate Committee on Homeland Security over the past two years. On June 9, 2010, the House of Representatives passed the Grid Reliability and Infrastructure Defense (GRID) Act (H.R. 5026).

The GRID Act would give FERC the authority to issue emergency orders to protect the bulk power

[30] U.S. Department of Energy Office of Inspector General Office of Audits and Inspections, *Audit Report Federal Energy Regulatory Commission's Monitoring of Power Grid Cyber Security*, 2011.
[31] NIST Smart Grid Collaboration Site, "Priority Action Plans," Accessed on December 28, 2010, <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WebHome#Priority_Action_Plans_PAPs>.
[32] ISO New England, *Overview of the Smart Grid—Policies, Initiatives and Needs*, ISO New England, February 17, 2009.
[33] GridWise, *Architecture Council Interoperability Constitution Whitepaper*, Gridwise, December 5 2006, accessed on December 28, 2010.
[34] Op Cit EISA 2007, subchapter IX.

system if a grid security threat is identified. Congress defined a grid security threat as "a substantial likelihood of:

> (A)(i) a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event, that could disrupt the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of the bulk power system or of defense critical electric infrastructure; and
>
> (ii) disruption of the operation of such devices or networks, with significant adverse effects on the reliability of the bulk power system or of defense critical electric infrastructure, as a result of such act or event; or
>
> (B)(i) a direct physical attack on the bulk power system or on defense critical electric infrastructure; and
>
> (ii) significant adverse effects on the reliability of the bulk power system or of defense critical electric infrastructure as a result of such physical attack."

The GRID Act also authorized FERC to develop regulations to address grid cyber security vulnerabilities, instead of having to wait for NERC to develop reliability standards that address the issue. Congress defined a grid security vulnerability as:

> "a weakness that, in the event of a malicious act using electronic communication or an electromagnetic pulse, would pose a substantial risk of disruption to the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of the bulk power system."[35]

The GRID Act is currently being considered by the Senate. On August 6, 2010, the GRID Act was reported favorably out of the Senate Energy and Natural Resources Committee, with only one substantial amendment. This version would authorize DOE to issue emergency orders if a grid security threat is identified instead of FERC. In summary, the GRID Act, if passed, would authorize FERC or DOE to take emergency actions to protect the bulk power system from cyber attack if a grid security threat or vulnerability is identified.

State Action

Much of the leadership on Smart Grid cyber security will have to come at the state level. As FERC has no jurisdiction over electricity facilities used in local distribution or transmission of electricity used for intrastate commerce, many of the policies related to Smart Grid implementation and security will fall wholly under the purview of state regulators. As noted above, the Smart Grid creates the potential for vulnerabilities in the bulk power systems that originate at the *local* level, and which are therefore not subject to FERC or NERC jurisdiction. This situation gives state and local authorities a greater degree of responsibility in setting grid-related security policies.

However, very few state Public Utility Commissions (PUCs) have published comprehensive Smart Grid security policies. An exception is the California PUC, which released a study in August 2010 entitled "PG&E Advanced Metering Assessment Report." The report assessed various aspects of the advanced metering interface for PG&E, one of the country's largest utilities. It contained an appraisal of PG&E's smart meter security standards,

[33] 111th Congress, 2D Session, *H.R. 5026*.

as laid out by PG&E itself. PG&E, which provides electricity and natural gas service to around 15 million people, based its own smart meter security standards on the "AMI System Security Requirements" developed by the Smart Grid industry's OpenSG AMI-SEC Task Force, mentioned above.[36] Although the report found that PG&E met the standards set out by the AMI-SEC Task Force, the review did not include observation or assessment of the actual implementation of the security plan, or the installation of smart meters, due to lack of time and resources.[37]

Given the lack of existing data on the level of state action and awareness with regard to Smart Grid cyber security, The Brookings Institution commissioned a survey, which was sent to Public Utility Commissions in all fifty states plus the District of Columbia. The survey, which can be found in Appendix II, attempted to gauge the attitudes of state utility regulators to the threat of Smart Grid cyber attack, as well as their responses to several proposals for increasing cyber security. In order to maximize the response rate and to obtain the most accurate responses possible, respondents were asked to participate on the condition of anonymity. Nevertheless, only seven of the 51 survey recipients responded. While this sample is not enough to draw statistically significant conclusions, it provided valuable insight into the views of several PUCs.[38]

Among those that did respond to the survey, there was a clear sense of uncertainty with regard to technological and jurisdictional issues related to national Smart Grid policy. The state PUCs that responded all agreed that there was at least a "moderate" threat of a Smart Grid-related cyber attack on local electricity distribution infrastructure (although the majority of respondents put the threat at a "serious" or "very serious" level). However, there were divergent opinions as to the exact nature and scope of that threat. The PUCs expressed skepticism that damage to physical equipment and infrastructure at the distribution level was a likely consequence of lax cyber security standards, and considered such events at the bulk power level even more remote. The most prevalent opinion was that such problems could be mitigated with proper implementation of system security measures.

The results showed a lack of consensus on appropriate cyber security measures, standards and implementation methods. With one exception, the PUCs agreed that "regulating the security of the electric grid" was part of their mandate. However, there were divergent responses as to actual steps taken to secure the grid. Only one respondent PUC requires its utilities to prepare specific cyber security plans, and none of the PUCs that responded to the Brookings survey require the utilities they regulate to meet the federal NERC cyber security standards for distribution infrastructure.

There was broad resistance among respondents to the suggestion of expanding federal involvement in state regulation of the electric power system to the distribution level. Respondents were generally opposed to congressional requirements for PUCs to implement NERC cyber security reliability standards for distribution-level infrastructure, although some of the resistance was qualified and supported the adoption of standards generally. For instance, most of the respondents supported mandatory adoption of the NIST-led Smart Grid Interoperability Panel's protocols, standards and requirements for all technology that connects to the Smart Grid (to include smart meters and smart appliances).

---

[36] Structure Consulting Group, *PG&E Advanced Metering Assessment Report Commissioned by the California Public Utilities Commission*. Structure Consulting Group, September 2, 2010, 22.

[37] Ibid.

[38] One inference that can perhaps be drawn from the low response rate is the lack of concrete policy action that has been taken at the state level.

In some cases, the issue of granting FERC the authority to intervene in the operations of, and to issue orders to, local distribution system operators was explicitly opposed. The reasoning for this opposition varied from simple objection to "orders" being issued by a higher authority, to the nature of the threats that would warrant FERC intervention (identity theft and privacy threats were specifically mentioned as instances where FERC "may not be the appropriate entity to regulate"), to a clear objection to the state-federal jurisdictional line being breached under any circumstances. Even where the PUCs expressed support for FERC intervention, this was limited to threats to the bulk power system or "large distribution" systems, or in one case was limited to FERC "emergency notices" of "imminent cyber security threats that have a substantial likelihood of causing a malicious act." In all cases, the respondent PUCs were resistant to suggestions of increased federal oversight and control with regard to cyber security.

Private Sector and Public-Private Partnerships

Several non-governmental organizations have been established to address the issues of advanced meter infrastructure (AMI) security. The Advanced Metering Infrastructure Security (AMI-SEC) Task Force, established under the UCA International Users Group, a nonprofit corporation focused on assisting users and vendors in the deployment of standards, has worked since 2007 to form consistent security guidelines for AMI. In a 2009 report prepared for AMI-SEC, the Advanced Security Acceleration Project - Smart Grid (ASAP-SG), a collaborative effort between EnerNex Corporation, several North American utilities, NIST and DOE, published the *Security Profile for Advanced Metering Infrastructure*. The document aims to present security concerns relevant to AMI and to provide guidance and security controls to organizations developing or implementing AMI solutions for the Smart Grid. ASAP-SG has also established a DOE-sponsored working group that has produced AMI and Automated Data Exchange security profiles for Smart Grid system architecture.

The ZigBee Alliance, an association of technology companies working together to develop open-standard wireless monitoring and control protocol, has also played a significant role in the development of standards for residential and commercial users of Smart Grid. In 2008, ZigBee released its Smart Energy Profile, which has been adopted by many in the Smart Grid industry as the standard communications language for AMI and metering through the home area networks (HAN). In January 2010, ZigBee Smart Energy 2.0, a wireless security architecture explicitly designed to protect customer data confidentiality, was included in the NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.[39]

[39] Office of the National Coordinator for Smart Grid Interoperability, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, National Institute for Science and Technology, January 2010. 57.

Conclusions and Recommendations

The majority of stakeholders involved in the implementation of the Smart Grid agree that there is some level of cyber security threat to the electricity system of the United States from malicious actors, from either inside or outside the country, and that this threat is likely to increase with greater penetration of Smart Grid infrastructure.

In general, the most visible action on Smart Grid cyber security policy is being taken at the national level. Policies and standards are in place and continue to be developed by the federal agencies concerned (DHS, FERC, NIST, NERC) with regard to the wholesale/bulk power system. NIST and NERC are taking the lead in this area, with continued development of cyber security standards and Priority Action Plans to which stakeholders and policymakers can refer in their discussions and which outline the manner in which Smart Grid infrastructure should be built. However, it is still too early to gauge the effectiveness of these standards. In particular, some in the utility industry are concerned that the Critical Infrastructure Protection standards are insufficient. There is also concern that progress in federal cyber security regulations is lagging progress in other aspects of Smart Grid policy, resulting in an increasing vulnerability gap.

There has been less progress on cyber security policymaking at the state and local level than at the federal level. The federal government must take some responsibility for this. It is part of the federal government's job to convene, collaborate and work with the states. Indeed, a situation in which states took leadership roles without coordinating with the federal government, and each other, would result in a patchwork of inefficient polices that would further expose the nation to cyber vulnerabilities.

Nevertheless, the results of the Brookings survey show that, in contrast to the federal government, many state and local level authorities, and the utilities they regulate, have yet to approach issues of Smart Grid cyber security at the distribution level with rigor and consistency. The lack of clear and coordinated action at the state level has implications for end-users, whose private information and homes could become the objects of attack, and for the national electric grid, which will become increasingly more vulnerable as unsecured smart meters provide multiple potential new points of access for would-be saboteurs.

Although there is agreement that the Smart Grid will entail new security concerns for the power system, Public Utility Commissions (PUCs) are wary of regulations which may result (either explicitly or in the course of their implementation) in greater federal oversight of their regulatory responsibilities. In addition to concern about

increased federal intervention in state electricity markets, PUCs are concerned about the impact that investment in secure Smart Grid infrastructure may have on consumer electricity prices and allowable costs. This is a legitimate concern, and one that the federal government must take into consideration when coordinating with the states on cyber security policy. Moreover, any effort to engage with stakeholders at the distribution level should acknowledge that there are many aspects of the power system at the local and municipal levels that are not subject to the oversight of PUCs. In such cases, the relevant authority is more likely to be a rural electricity cooperative or a municipal utility. Any increased effort by the federal government to engage with distribution-level stakeholders should also include representatives from the private sector, which will be an important part of the transition to Smart Grid, particularly in measures that pertain to the development of AMI.

In light of the above conclusions, there are several steps which will facilitate the implementation of the Smart Grid throughout the United States.

1. NIST should complete its work on the 18 Priority Action Plans and the Smart Grid Interoperability Panel as soon as practicable. A set of approved and well-defined standards for security technologies will be critical to the successful and secure implementation of the Smart Grid.

2. Federal agencies should integrate PUCs, utilities and local level power-sector entities not subject to PUC authority into the process of standards and procedures development so that the limits of federal authority are clear and concerns of those at the distribution-level can be heard and integrated.

3. Federal agencies must strive to develop, in partnership with PUCs, utilities and local level entities not subject to PUC authority, security and interoperability standards for the distribution level electric grid.

4. Each state PUC, in collaboration with its associated utilities and Smart Grid vendors, should formulate and make available to the public a comprehensive Smart Grid cyber security plan. Where possible, PUCs should collaborate with each other to ensure that policies and procedures are harmonized.

Smart Grid security is a rapidly changing field and must be thought of as a work in progress. Implementation will be an iterative process, with perfect security an unattainable goal, just as perfect security is not now a reality. Expectations must be of a slow but meaningful path forward to better and better Smart Grid security. It is incumbent upon those responsible for implementation of the Smart Grid to see that sufficient cyber security steps are taken to protect customer information and privacy, as well as the integrity of the electrical grid itself, during the build out phase of the Smart Grid. It is clear that there is much common ground to build on regarding many of the issues surrounding Smart Grid cyber security. The actions taken by the federal government show a recognition of the issue at the national level. However, involvement of state and local-level actors is imperative to the development of a Smart Grid system that works. Failure to cooperate on this issue could see the piecemeal development of Smart Grid security standards, and the inability of grid security systems to work together to combat penetration by malicious actors. The Smart Grid offers the United States the potential for significant economic, environmental and energy security benefits. However, without strong, coordinated policies to ensure system-wide cyber security, these benefits may be greatly diminished.

Appendix I

DOE Smart Grid Systems Report Summary of Smart Grid Metrics and Status				
Number	Metric Title	Type	Penetration/ Maturity	Trend
	Area, Regional and National Coordination Regime			
1	Dynamic Pricing: fraction of customers and total load served by RTP, CPP, and TOU tariffs	build	low	moderate
2	Real-time System Operations Data Sharing: Total SCADA points shared and fraction of phasor measurements points shared	build	moderate	moderate
3	Distributed-Resource Interconnection Policy: percentage of utilities with standard distributed-resource interconnection policies and commonality of such polices across utilities	build	moderate	moderate
4	Policy/Regulatory Progress: weighted-average percentage of smart grid investment recovered through rates	build	low	moderate
	Distributed-Energy-Resource Technology			
5	Load Participation Based on Grid Conditions: fraction of load served by interruptible tariffs, direct load control, and consumer load control with incentives	build	low	Low
6	Load Served by Microgrids: the percentage of total grid summer capacity	build	nascent	Low
7	Grid-Connected Distributed Generation (renewable and non-renewable) and Storage: percentage of distributed generation and storage	build	low	high
8	EVs and PHEVs: percentage shares of on-road, light-duty vehicles comprising of EVs and PHEVs	build	nascent	Low
9	Grid-Responsive Non-Generating Demand-Side Equipment: total load served by smart, grid-responsible equipment	build	nascent	Low
	Delivery (T&D) Infrastructure			
10	T&D Reliability: SAIDI, SAIFI, MAIFI	value	mature	declining
11	T&D Automation: percentage of substations using automation	build	moderate	high
12	Advanced Meters: percentage of total demand served by advanced metered (AMI) customers	build	low	high
13	Advanced System Measurement: percentage of substations possessing advanced measurement technology	build	low	moderate
14	Capacity Factors: yearly average and peak-generation capacity factor	value	mature	flat
15	Generation and T&D Efficiencies: percentage of energy consumed to generate electricity that is not lost	value	mature	improving
16	Dynamic Line Ratings: percentage miles of transmission circuits being operated under dynamic line ratings	build	nascent	Low
17	Power Quality: percentage of customer complaints related to power quality issues, excluding outages	value	mature	declining
	Information Networks and Finance			
18	Cyber Security: percent of total generation capacity under companies in compliance with NERC Critical Infrastructure Protection standards	build	nascent	nascent
19	Open Architecture/Standards: Interoperability Maturity Level - the weighted average maturity level of interoperability realized among electricity system stakeholders	build	nascent	nascent
20	Venture Capital: total annual venture-capital funding of Smart Grid startups in the United States	value	nascent	high

Appendix II

SMART GRID SECURITY WHITE PAPER SURVEY

The Threat

1. How serious do you consider the threat of a Smart Grid related cyber attack on a local distribution system?

   a. Very Serious ☐
   b. Serious ☐
   c. Moderate ☐
   d. Not Serious ☐
   e. Not an Issue ☐

2. Do you believe it is possible to cause serious damage to a local distribution system through a Smart Grid related cyber attack? Serious damage is defined as a brownout, blackout or other loss of electricity, or destruction of electricity distribution, transmission or generating equipment.

   Yes ☐ No ☐

3. Do you believe it is possible to attack the bulk power system through a Smart Grid-related cyber attack?

   Yes ☐ No ☐

4. Do you believe it is possible to cause serious damage to the bulk power system through a Smart Grid-related cyber attack?

   Yes ☐ No ☐

5. Do you believe you have been given enough information by the federal intelligence community to properly evaluate threats associated with smart grid security?

   Yes ☐ No ☐

State Action

6. Do you consider regulating the security of the electric grid to be part of your mandate?

   Yes ☐ No ☐

7. Do you require the electric utilities you regulate to adopt the NERC cyber security reliability standards (CIP 002-009) for local distribution infrastructure?

   Yes ☐ No ☐

8. Do you require the electric utilities you regulate to prepare cyber security plans?

   Yes ☐ No ☐

9. Have you taken additional action(s) to address cyber security threats? If yes, please elaborate below.

   Yes ☐ No ☐

10. Do you allow the utilities you regulate to recoup the investments they make in cyber security in their rate base?

    Yes ☐ No ☐

Federal Action

11. Should Congress require electric utilities to implement the NERC cyber security reliability standards for local distribution infrastructure?

    Yes ☐ No ☐

12. Do you believe that the protocols, standards and requirements to address Smart Grid cyber security risk areas that are being developed by the NIST-led Smart Grid Interoperability Panel should be mandatory for all technology that connects to the smart grid, including all local distribution system equipment, smart meters and any "smart appliance"?

    Yes ☐ No ☐

13. Should FERC have authority to issue emergency orders to operators of the local distribution systems of the electric grid if a cyber security threat is identified? A cyber security threat is defined as a "substantial likelihood of a malicious act using electronic communication…that could disrupt the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of the bulk power system …; and disruption of the operation of such devices or networks, with significant adverse effects on the reliability of the bulk power system.., as a result of such act or event."

    Yes ☐ No ☐

14. Do you believe that FERC should have authority to issue emergency orders to operators of the local distribution system of the electric grid if a cyber security vulnerability is identified? A cyber security vulnerability is defined as "a weakness that, in the event of a malicious act using electronic communication…, would pose a substantial risk of disruption to the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of the bulk power system."

Yes ☐ No ☐

BROOKINGS
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, D.C. 20036
brookings.edu