

Chapter 9: Data Communications, Cybersecurity, and Information Privacy

In this chapter, we discuss the opportunities associated with expanded data communications capabilities throughout the electric grid and the related cybersecurity and information privacy challenges.

Section 9.1 describes the evolution of grid communications systems and discusses the interoperability and network ownership challenges posed by expanded communications. Data communications will increasingly link the various components of the grid, from generator to transmission line to substation to distribution network to consumer meter, and to equipment and appliances within homes and businesses. As communications needs and technologies continue to change, the industry will have to deal with a state of “continuous transition” unlike anything it has seen before. This discussion serves as important background for our recommendations related to cybersecurity and information privacy.

Section 9.2 is an examination of cybersecurity issues facing networked grid systems and related regulatory developments. Ongoing cybersecurity standards development processes are critical to securing the grid. However, it will be impossible to fully protect the grid from cyber accident or attack, and response and recovery mechanisms that reduce the impact of these events need to be investigated and promulgated throughout the industry. While the North American Electric Reliability Corporation has developed Cybersecurity Infrastructure Protection standards covering the bulk power system, and the National Institute of Standards and Technology is coordinating the development of a standards framework across a large group of industry, academic, and government participants, no organization currently has responsibility for overseeing grid cybersecurity across all aspects of grid operations.

In Section 9.3 we examine the information privacy issues related to expanded operational and consumer data collection, storage, use, and disclosure. Consumers have raised these issues and state PUCs are responding by creating various regulations regarding the protection and use of consumer electric usage data (CEUD). With companies working in multiple states and data crossing state boundaries, further coordination among these agencies will be needed to ensure the public that data collection in the future grid is appropriately protected.

We conclude, in Section 9.4, with a set of recommendations. We highlight the importance of existing industry-government partnerships that are working towards establishing comprehensive interoperability standards. We also recommend the designation of a single agency with responsibility for cybersecurity preparedness, response, and recovery throughout the entire grid. Finally, we recommend that state agencies and other stakeholders focus on coordinating their efforts related to data privacy.

The electric grid is a “system of systems,” managed by thousands of people, computers and manual controls, with data supplied by tens of thousands of sensors connected by a wide variety of communications networks. Over the next 20 years, the growth in percentage terms of data flowing through grid communications networks will far exceed the growth of

electricity flowing through the grid. Many advances discussed in this study—from integration of variable energy resources to wide-area situational awareness and real-time control to demand response—result from or depend on this increase in data collection and communications.

Critical challenges will arise from the expansion of existing communications flows and the introduction of new ones, some of which are illustrated in Figure 9.1.

While the increase in data communications will bring significant benefits, it also will give rise to new costs and challenges. Beyond the direct costs of hardware, software, networks, and staff, significant additional costs may arise from the

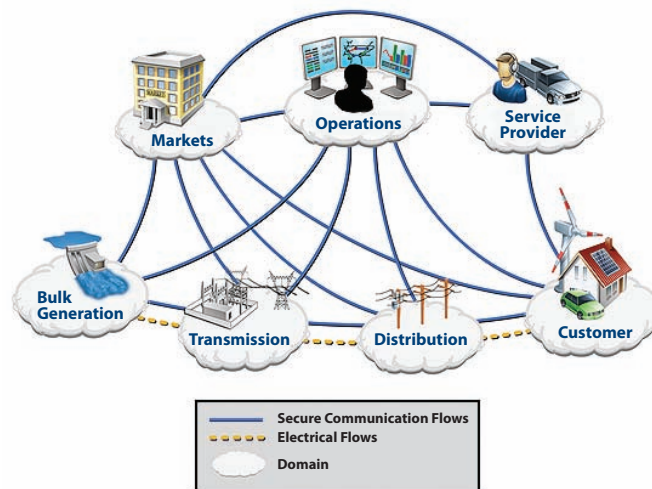
complicating the cost–benefit analysis of spending to protect communications systems.

In addition, the highly interconnected grid communications networks of the future will have vulnerabilities that may not be present in today’s grid. Millions of new communicating electronic devices, from automated meters to synchrophasors, will introduce attack vectors—paths that attackers can use to gain access to computer systems or other communicating equipment—that increase the risk of intentional and accidental communications disruptions.¹ As the North American Electric Reliability Corporation (NERC) notes, these disruptions can result in a range of failures, including loss of control over grid devices, loss of communications between grid entities or control centers, or blackouts.²

The highly interconnected grid communications networks of the future will have vulnerabilities that may not be present in today’s grid.

improper or illegal use of data and communications. Unfortunately, these costs are difficult to quantify and can only be discussed in terms of probabilities and estimates of potential impact to businesses and consumers,

Figure 9.1 Diagram of the Future Electric Grid, Showing Communications and Power Flows



Source: National Institute for Standards and Technology, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, special publication 1108 (Washington, DC: U.S. Department of Commerce, 2010), 33, http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

Making sound decisions regarding cybersecurity, from attack prevention, response, and recovery to information privacy, requires confronting a number of very basic societal and economic questions. As listed in a report by NERC and the U.S. Department of Energy (DOE),³ these include:

- How much risk is the private sector willing to accept?
- How much risk is the public sector willing to accept?
- How much are consumers (or society at large) willing to pay to reduce this risk?
- Who makes the determination of society's tolerance for risk and the cost of employing protections?
- How should the costs of employing protections be paid for?
- How is damage measured: cost to replace damaged equipment, number of people-hours without power, number of other critical infrastructure nodes affected?
- Where are interdependencies most critical?

To contribute to this discussion, this chapter examines critical topics and strategies to increase awareness and resolution of cybersecurity and information privacy issues in the future electric grid.

9.1 GRID DATA COMMUNICATIONS

Several types of data communications networks already serve many purposes in the electric grid:

- **Utility-owned wide-area and field-area networks** send and receive operational measurement and control signals between control centers, substations, and sensors along transmission lines and the distribution network. They rely on wired (fiber and copper), wireless (cellular), and radio-frequency or microwave communications.
- **Commercial wide-area, field-area, and local (neighborhood) networks** are used for similar purposes to utility-owned networks as well as for communications among corporate data centers. They rely on wired, wireless, radio-frequency or microwave, and power line carrier communications, provided under contract or operating arrangements from common public telecommunications service providers.
- **Public communications networks**, such as the telephone network and the Internet, transmit information, such as pricing signals and daily generation schedules, and communicate with home energy networks.
- **Satellite communications networks** are used where microwave communication is prohibitively expensive; phasor measurement units (PMUs) also use the GPS satellite navigation system to synchronize timing.
- **Home and commercial premises networks** connect appliances and transmit control information from utilities to homes or businesses and are typically provided by the customer.

Table 9.1 illustrates the growing use of data communications in the grid and lists the changes that have occurred in network architectures, media, and protocols over the past 25 years. These changes follow the general evolution of computer and communication technologies and can be expected to continue far into the future. Ensuring that grid communications networks are accurate, reliable, and economical in this constantly changing environment is one challenge to achieving the goals of the future electric grid.

Future Data Communications Architecture

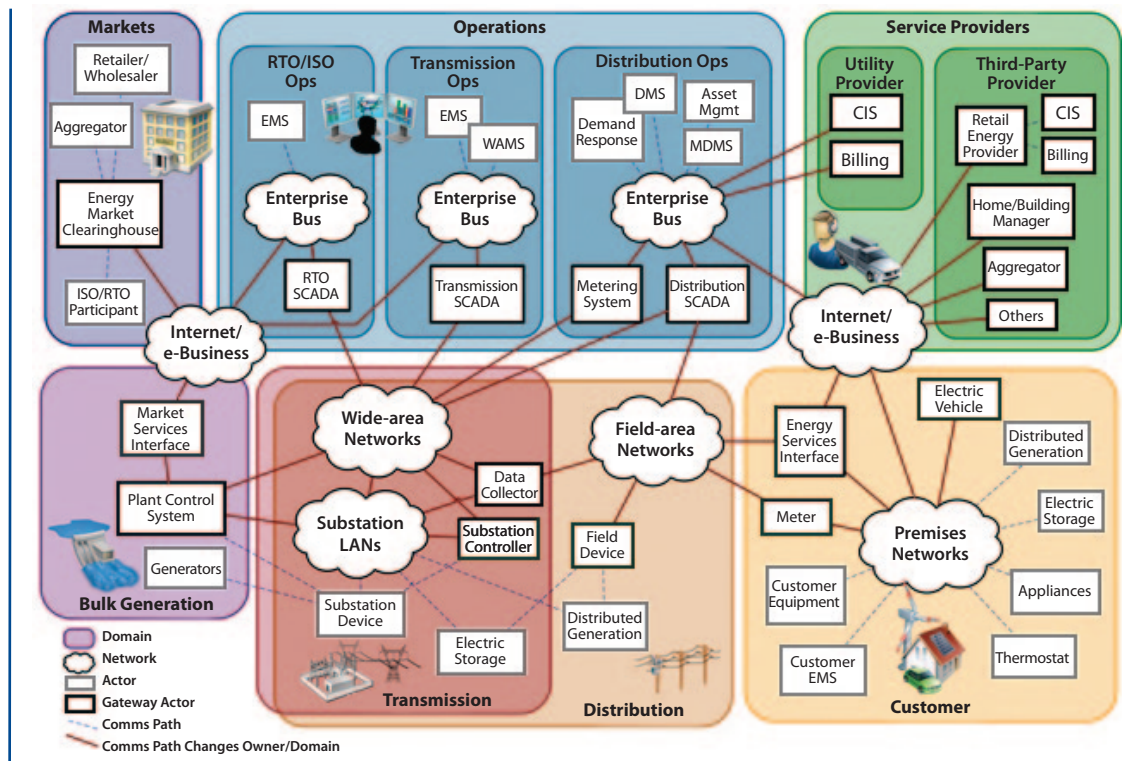
Research projects investigating the future architecture of data communications networks highlight that they will closely link generators, transmission networks, substations, local data collectors, smart meters and appliances, and other grid components using two-way and broadcast communications.⁴ In addition, market operators, corporate offices, utility back-office systems, and utility planning systems will be connected with a more flexible, more reliable, and faster communications infrastructure. Figure 9.2 is a conceptual representation of the future of interconnected communications across the electric grid.

Table 9.1 Summary of Communications System Development for Electric Utilities

Phase	Years	System Characteristics	Network Architecture	Communication Media	Communication Protocols and Standards
Nonstandardized	Up to 1985	<ul style="list-style-type: none"> • Many proprietary systems • Single vendor per system • Basic data collection 	<ul style="list-style-type: none"> • Hierarchical tree • Single master • Isolated substations 	<ul style="list-style-type: none"> • RS232 and RS485 • Dial up • Trunked radio • Power line carrier • Less than 1,200 bytes per second (bps) 	<ul style="list-style-type: none"> • Modbus • SEL • WISP • Conitel 2020
Standards Development Begins	1985–1995	<ul style="list-style-type: none"> • Multivendor systems • Protocol conversion 	<ul style="list-style-type: none"> • Hierarchical tree • Multiple masters • Redundant links 	<ul style="list-style-type: none"> • Leased lines • Packet radio • 9,600 to 19,200 bps 	<ul style="list-style-type: none"> • DNP3 Serial • IEC 60870 • TASE 2
Local-area Networks (LANs) and Wide-area Networks (WANs)	1995–2000	<ul style="list-style-type: none"> • Introduction of LANs in substations • Merging protection and SCADA networks 	<ul style="list-style-type: none"> • Peer-to-peer communication in substation • Joining substations via WAN 	<ul style="list-style-type: none"> • Ethernet • Spread spectrum radio • Frame relay • Megabit data rates 	<ul style="list-style-type: none"> • TCP-IP • FTP • Telnet • HTTP • DNP3 WAN/LAN • UCA 2.0
Integration into Business	2000–present	<ul style="list-style-type: none"> • Merging automation and business networks • Corporate IT departments • Asset management 	<ul style="list-style-type: none"> • Linking of utility WAN to corporate network • Extension of network to customer premises • Use of Internet 	<ul style="list-style-type: none"> • Digital cellular • IP radios • Wireless ethernet • Gigabit backbones 	<ul style="list-style-type: none"> • TCP-IP • IEC 61850 • XML

Source: V. C. Gungor and F. C. Lambert, “A Survey on Communication Networks for Electric System Automation,” *Computer Networks* 50, 7 (2006): 877–97.

Figure 9.2 Detailed Communications Flows in the Future Electric Grid



Source: National Institute for Standards and Technology, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, special publication 1108 (Washington, DC: U.S. Department of Commerce, 2010), 35, http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

Note: ISO/RTO = independent system operator/regional transmission organization; EMS = energy management system; SCADA = supervisory control and data acquisition; WAMS = wide-area management system; DMS = distribution management system; MDMS = meter data management system; CIS = customer information system; LAN = local-area network.

An important issue in the management and regulation of grid data communications systems will be the blurring of distinctions

Existing point-to-point and one-way communications networks will need to be expanded or replaced with networks designed for two-way communication.

between “generators” and “consumers,” particularly as consumers who previously only consumed electricity begin participating in demand response programs and generating their own electricity through fuel cells, wind turbines, solar roofs, and the like. Data

communications systems will need to enable customers to perform these multiple roles. As the grid evolves, the existing point-to-point and one-way communications networks will need to be expanded or replaced with networks designed for two-way communication.⁵

Data Communications Technologies and Applications

The new grid technologies discussed in this study will generate large amounts of data very rapidly, which will necessitate data communications networks with increased capacity, reduced latency (delay in transmitting and receiving), and higher reliability than is required today. A 2007 National Energy Technology Laboratory

report for the DOE recognized these increased needs, finding that “the communications systems utilized in the power industry today are too slow and localized to support the integrated communications needed to enable the modern power grid.”⁶ Better data storage and management, and more systems to process and use the data, also are needed. Managing diverse computer and communications technologies will pose technical challenges for utility engineers and policy challenges for regulators.

Table 9.2 lists data and network requirements associated with various grid applications. These estimates are from industry sources and include subjective and objective measures. While valuable in providing an overall picture of communications needs, they must be examined carefully for any specific use. Consider the example of reliability requirements, which range from 99% (3.65 days of outage per year) to 99.9999% (31 seconds per year). Not only are these ranges considerable, but they do not show the impact over long or short time periods. A single three-day outage of an advanced metering infrastructure (AMI) system during a hot summer month could eliminate the entire value of a demand response system, whereas multiple short outages in other seasons totaling three days might have little impact. Data rate and latency estimates also have relatively broad ranges. In general, all these estimates show the need for significant expansion and improvement in data communications capabilities.

Individual home networks, which monitor and control appliances and HVAC, have the least stringent requirements, and these networks will most likely be provided by consumers rather than utilities. The bandwidth requirements for

AMI data communications are also relatively low at the source—tens of kilobytes per second for individual meters to 100 kilobytes per second for concentrators and access control points. In the aggregate, AMI systems can generate in the range of 1 gigabyte of data per day per million meters, or as much as 1–2 terabytes per year for a major utility, a significant but not overwhelming amount of data. Whether AMI systems transmit even more data in the future will depend on the requirements of demand response and other future applications.

On the other hand, wide-area monitoring systems for more advanced control of the distribution and transmission grids will collect operational parameters—for example, voltage, current, phase, and frequency—at a subsecond rate and transmit these data to grid operation centers for immediate processing and action. These systems will require high data transfer rates with high reliability as well as backup power and other redundancies.

Designing future grid communication networks to meet these network requirements will take creative technical solutions and collaboration among utilities, vendors, systems integrators, and customers. The industry already is working to explore many different system design trade-offs. Most of these decisions will not require direct government input. However, policy makers can make important contributions to two areas of significant debate: standards and interoperability, and ownership of data communications networks. These challenges are discussed in the next two sections.

Table 9.2 Current and Potential Grid Communications Use

Application	Media	Standard/ Protocol	Network Requirements						
			Expected Data Rate/Bandwidth ^a	Acceptable Latency ^a	Frequency of Use ^b	Reliability Need ^a	Security Need ^a	Backup Power ^a	
Home-area Network	Power line communications; ^c wireless	HomePlug, ZigBee, IP							
Advanced Metering Infrastructure (AMI)*	Power line communications; ^{c,d} wireless radio frequency; ^{e,f} T1, microwave, broadband (via fiber, cable, digital subscriber line), commercial wireless ^g	For backhaul: WiMAX, LTE For appliance to meter: IEEE 802.15.4, ^h ZigBee ^g	10–100 kilobytes/second (kbps)/node, 500 kbps for backhaul	2–15 seconds	5–15 minutes/node	99–99.99%	High	Not necessary	
Demand Response (Part of AMI)	Same as AMI	Same as AMI	14 kbps–100 kbps/node or device	500 milliseconds (ms)–several minutes	35 days/year	99–99.99%	High	Not necessary	
Electric Transportation	Power line communications ⁱ wireless ^h	ZigBee, IEEE 802.15.4 ^h	9.6–56 kbps, 100 kbps is a good target	2 seconds–5 minutes	Daily	99–99.99%	Relatively high	Not necessary	
Distribution Grid Management	Fiber, wireless, ^j satellite, cellular ^g	DNP3 (IEEE 1815), IEC 61850/GOOSE, ^k WiMAX, LTE, ^j IP, ^g IEEE 802.15.4 ^h	9.6–100 kbps	100 ms–2 seconds	Continuous	99–99.999%	High	24–72 hours	
Distributed Energy Resources and Storage	Fiber, wireless, ^j microwave, satellite ^g	DNP3, IEC 61850/GOOSE ^k WiMAX, LTE, ^j ZigBee, ^g IEEE 802.15.4 ^h	9.6–56 kbps	20 ms–15 seconds	Continuous	99–99.99%	High	1 hour	
Wide-area Situational Awareness (synchrophasors [#])	SONET, ATM, Frame Relay, MPLS, ^{f,g} fiber, microwave, broadband over power line ^g	C37.118, IEC 61850/GOOSE, ^k IP ^{h,i}	600–1,500 kbps	20 ms–200 ms	Continuous	99.999–99.9999%	High	24-hour supply	
Interutility communications (Southern California Edison)	Fiber, microwave, wired	ICCP ^k	> 45 megabytes/second (mbps)	<50 ms (DS-3)	Continuous	99.999–99.9999%	High	24-hour supply	
Interregional data communications (ISO New England)	Standard telco T1 circuits with copper endpoints (NERCNet)	IP	256 kbps	20–200 ms	Continuous	99.999%	High	24-hour supply	
Market data communications (ISO New England)	Wired	IP	18 mbps + 45 mbps connections	20–200 ms	Continuous	99.999%	Relatively high	24-hour supply	

Notes:

* Communications between the utility and smart meters have different requirements than those between smart meters and appliances, although these are sometimes lumped under the category “advanced metering infrastructure.” While the former necessitate reliable communications over long distances, the latter necessitates low latency over short distances.

A significant synchrophasor initiative is the North American SynchroPhasor Initiative. A communications network called NASPINet to support these technologies is under construction. More information may be found at <http://www.naspi.org>.

^aIndicated column in source table from: U.S. Department of Energy, *Communications Requirements of Smart Grid Technologies, Appendix A* (Washington, DC, 2010), http://www.doe.gov/sites/prod/files/gcprod/documents/Smart_Grid_Communications_Requirements_Report_10-05-2010.pdf.

^b“Frequency” developed from: U.S. Department of Energy, *Communications Requirements of Smart Grid Technologies, Appendix A* (Washington, DC, 2010), http://www.doe.gov/sites/prod/files/gcprod/documents/Smart_Grid_Communications_Requirements_Report_10-05-2010.pdf.

^cN. Pavlidou, A. J. Han Vinck, J. Yazdani, B. Honary, “Power line communications: State of the Art and Future Trends,” *IEEE Communications Magazine* 41, 4 (April 2003): 34–40.

^dEDN Europe, “Maxim and Sagem to Develop Power-Line Comms for EDF,” press release, December, 12, 2008, <http://www.edn-europe.com/maximsagemtodeveloppowerlinecommsforedf+article+2679+Europe.html>.

^eV. C. Gungor and F. C. Lambert, “A Survey on Communication Networks for Electric System Automation,” *Computer Networks* 50, 7 (2006): 877–97.

^fM. McGranaghan, D. Von Dollen, P. Myrda, and E. Gunther, “Utility Experience with Developing a Smart Grid Roadmap,” presentation at IEEE Power and Energy Society General Meeting, Pittsburgh, PA, July 20–24, 2008.

^gU.S. Department of Energy, *Communications Requirements of Smart Grid Technologies: Department of Energy* (Washington, DC, 2010), http://energy.gov/sites/prod/files/gcprod/documents/Smart_Grid_Communications_Requirements_Report_10-05-2010.pdf.

^hPersonal communication with Exelon Staff, April 25, 2011.

ⁱRenault Nissan, “Renault and EDF Strengthen Collaboration on Zero-Emission Electric Vehicle,” press release, June 22, 2009, http://www.media.renault.com/download/media/specialfile/9210_1_5.aspx.

^jV. K. Sood, D. Fischer, J. M. Eklund, and T. Brown, “Developing a Communication Infrastructure for the Smart Grid,” presentation at IEEE Electrical Power & Energy Conference, Montreal, QC, Canada, October 22–23, 2009.

^kPersonal communication with Southern California Edison Staff, March 15, 2011.

^lQualityLogic, “IEEE C37.118 PMU Communications,” http://www.qualitylogic.com/Contents/Smart-Grid/Technology/IEEE-C37_118.aspx.

Standards and Interoperability

As more components are introduced into the communications infrastructure, ensuring interoperability among communications devices via standardized communications protocols and other interface standards will be critical.⁷ The U.S. National Institute of Standards and Technology (NIST) Cybersecurity Working Group identified 137 interfaces between different grid systems.⁸ For example, every smart meter and most sensors and major pieces of equipment at generating plants and substations will have communications modules—using millions of components from potentially hundreds of manufacturers. Software applications will similarly be provided by different developers. After installation, the technologies of the communications infrastructure will continue to evolve, requiring ongoing interoperability assessments and review. “Backward compatibility” will be required since newer equipment will have to operate alongside older equipment, even though this may decrease the functionality available.

From a cybersecurity perspective, interfacing so many different hardware and software components introduces vulnerabilities—especially when new and legacy hardware and software need to operate together. For example, implementing customer demand response involves power flow management at the distribution level, interfacing AMI, distribution grid management systems, and billing systems across large numbers of customers, not all of whom will have installed equipment from the same manufacturer, or even the same generation of equipment. The presence of so many interfaced components increases system complexity as well as the number of potential cyber vulnerabilities.

Standardization around a set of communications protocols is critical to achieving interoperability. Communications protocols are the rules and formats for communicating digital data. The protocol in conjunction with the communications media in large measure determines the data rate, latency, security, and reliability of the communications network. The 2007 National Energy Technology Laboratory report prescribes “an open communications architecture that

Standardization around a set of communications protocols is critical to achieving interoperability.

supports ‘plug and play’ interoperability” and “universally accepted standards for these communications...defined and agreed upon in the industry.”⁹ NIST has tackled this problem by organizing a public–private partnership, the Smart Grid Interoperability Panel (SGIP), to identify standards for the grid as well as address gaps where standards are lacking; the first version of the resulting NIST report was published in 2010.¹⁰ The second version became available for public comment October 25, 2011. Trading off the deployment of new technologies against interoperability requirements will become a major challenge for utility engineers.

Several debates over protocol choice are ongoing. For example, the successful deployments of new devices in locations that wired communications cannot reach economically can only be achieved with secure, wide-area, broadband wireless communications; two important wireless communications protocols are Worldwide Interoperability for Microwave Access (WiMAX) and Long Term Evolution (LTE), although momentum is clearly on the side of LTE. The home-area network industry is also debating different protocols for communicating among appliances and smart meters, including ZigBee, Inseon, Z-Wave, and X10. While the ZigBee protocol appears to have the most momentum in this area, other protocols cannot yet be ruled out.

Internet Protocol (IP) is the core protocol of the public Internet, defining the message formats for transmitting data across networks. Because IP is already used almost universally, commercially available software and hardware systems are designed to process IP traffic and protect IP-based networks from intrusion, thus making IP the obvious choice for most networking applications.ⁱ In July 2011, NIST's Smart Grid Interoperability Panel plenary session formally approved a set of IP protocols, outlined in the document "Internet Protocols for the Smart Grid," for use in the grid.¹¹ Indeed, IP is already in use in the grid, and IP-based networks are predicted to be important for a number of smart-grid and other future applications.¹² DOE also has received recommendations from several utility and telecommunications industry representatives that grid communications be standardized on IP. While some application-specific protocols may have better characteristics in limited cases, IP may quickly become an important protocol of choice for general deployment.ⁱⁱ

Independence and Security Act of 2007 gives FERC responsibility for "adopting" standards recommended by NIST, but it is unclear how that responsibility will be used.¹⁴ At this stage, FERC has determined that there is not sufficient consensus regarding these standards and declined to adopt them. Other groups support this decision. The National Science and Technology Council suggests that "embracing standards as best practices in the field" rather than requiring mandatory adoption will be sufficient to ensure the development of the future grid.¹⁵ The Electric Power Research Institute (EPRI) adds that "consensus-based standards deliver better results over [time]."¹⁶ Additionally, the U.S. Government Accountability Office (GAO) finds that FERC lacks an approach to monitor industry compliance with any related standards it adopts in this process.¹⁷

The key trade-off is between early standardization (which may limit innovation) and late standardization (which may delay adoption and lead to future interoperability problems). In the short run, NIST's facilitation of recommended standards will encourage market entry and facilitate interoperability. The fundamental question is how to ensure that innovation continues in and around the standardization process. The imposition of detailed federal standards beyond what comes out of this process would not appear to be productive, although federal agencies, state public utility commissions (PUCs), utilities, and consumer groups each have important roles to play as participants in the standard-setting process.

Decisions to standardize on specific protocols require input from a wide range of industry stakeholders, and federal agencies play an important convening role.

Decisions to standardize on specific protocols require input from a wide range of industry stakeholders, and federal agencies play an important convening role. For example, the NIST identified five standards for the Federal Energy Regulatory Commission's (FERC) consideration in October 2010.¹³ The Energy

ⁱ It is important to note that the use of IP for grid data communications is not the same as using the public Internet. In most cases, the discussion of IP networks for grid communications envisions fully separate networks that are not connected to the public Internet, although some data communications applications do envision using the public Internet. These are separate debates. For the electric grid, it will be vital to keep critical grid communications systems from "talking" to the public Internet and becoming infected as a result.

ⁱⁱ Even this should be viewed as an evolving situation, although changes may be a decade or more away. For example, the National Science Foundation supports a Global Environment for Network Innovations program, which aims to design protocols that can run on the Internet in parallel with IP to reduce latency and improve security for future applications (see <http://www.geni.net/>).

FINDING

The ability of utilities to incorporate technological developments in electric grid systems and components on an ongoing basis will be critical to mitigating the data communications and cybersecurity challenges associated with grid modernization. Development and selection processes for interoperability standards must strike a balance between allowing more rapid adoption of new technologies (early standardization) and enabling continuous innovation (late standardization).

Ownership of Data Communications Networks

The ownership of grid data communications networks is also the subject of significant debate. At issue is whether to base future grid communications on utility-owned private networks or facilities operated by or leased from telecommunications companies. Traditionally, utilities have built private networks to support applications with critical latency, reliability, and security requirements and used commercial ones for applications with less stringent requirements.

Ultimately, the choice depends on the assessment each company makes about cost (capital versus operating, often treated differently in utility regulation), reliability, availability, and control. Utilities cite all factors as justifying direct ownership; for example, integrated utilities claim that during emergencies, commercial

networks will be flooded with traffic and possibly become unusable by utilities that would have to compete for access to the networks.¹⁸ Using public communications networks in the electric grid also establishes more interdependencies between the telecommunications and electric power industries, which could pose security and reliability problems, for example, by increasing the vulnerability of both industries to cascading failures that spill over from one industry to another.¹⁹

Telecommunications companies, on the other hand, maintain that commercial networks can satisfy the requirements of the grid.²⁰ The Federal Communications Commission (FCC) has stated that because “97.8% of Americans are already covered by at least one 3G network, a hardened commercial wireless data network could serve as a core part of the Smart Grid.”²¹ The FCC wants to begin testing the reliability and resilience of these networks and has

At issue is whether to base future grid communications on utility-owned private networks or facilities operated by or leased from telecommunications companies.

recommended that states reduce disincentives to using them for grid communications. However, it does not ultimately endorse one specific ownership model over another, recognizing that specific circumstances must be taken into account.ⁱⁱⁱ Further, no study provides definitive data to fully support either approach, which leads to the conclusion that opportunities exist for both utility-owned and commercial networks in a regulatory environment that encourages both equally.

ⁱⁱⁱ In its National Broadband Plan, the FCC makes the following recommendations on the issue of grid data communications network ownership: “The country should pursue three parallel paths. First, existing commercial mobile networks should be hardened to support mission-critical Smart Grid applications. Second, utilities should be able to share the public safety mobile broadband network for mission-critical communications. Third, utilities should be empowered to construct and operate their own mission-critical broadband networks. Each approach has significant benefits and trade-offs, and what works in one geographic area or regulatory regime may not work as well in another. Rather than force a single solution, these recommendations will accelerate all three approaches.”²²

A related regulatory issue is the allocation of spectrum for utility communications. Utilities currently use licensed and unlicensed spectrum

A related regulatory issue is the allocation of spectrum for utility communications.

that is shared with other users and uses. The choice of spectrum often depends on the specific application and features of the service territory—for instance, in rural areas interference is less of an issue than in urban areas.²³ While these considerations have historically dominated utilities' thinking about spectrum, the utilities are increasingly focused on how they will get access to spectrum during emergencies. One of the questions being debated is whether utilities should share networks with public safety users—police, firefighters, and ambulance technicians—or have separate spectrum. In its National Broadband Plan, the FCC recommends that Congress consider amending the Communications Act of 1934 to allow utilities to use the public safety network in the 700 megahertz band and that the National Telecommunications and Information Administration and FCC continue to identify new uses for federal spectrum, especially with respect to the smart grid.²⁴

In contrast, American Electric Power, Utilities Telecom Council, and other major electricity companies and utility trade groups support dedicated wireless spectrum for utilities' exclusive use, arguing that it will facilitate grid development.²⁵ Resolution of this question by the FCC requires considering the role of electricity service in servicing all other public safety users, particularly in times of natural or other disaster, and how that is best accomplished.

9.2 CYBERSECURITY OF THE ELECTRIC GRID

Cybersecurity refers to all the approaches taken to protect data, systems, and networks from deliberate attack as well as accidental compromise, ranging from preparedness to recovery. Increased data communications throughout the electric grid will introduce new cybersecurity risks and challenges, to both local and wide-scale grid systems. Some examples follow:

- **Loss of grid control** resulting in complete disruption of electricity supply over a wide area can occur as a result of errors or tampering with data communication among control equipment and central offices.
- **Consumer-level problems** ranging from incorrect billing to interruption in electric service can be introduced via smart meter tampering.
- **Commuting disruptions** for electric vehicle operators can occur if recharging stations have been modified to incorrectly charge batteries.
- **Data confidentiality breaches**, both personal and corporate, can provide information for identity theft, corporate espionage, physical security threats (for example, through knowing which homes are vacant), and terrorist activities (for example, through knowing which power lines are most important in electric distribution).

As observers from industry, government, and academia have recognized, the need to mitigate such risks makes grid cybersecurity an important concern for society at large as well as for individual companies. For example, the 2009 NERC Long-term Reliability Assessment includes cybersecurity as one of six issues projected to be of high likelihood and consequence within 10 years.²⁶ For the grid, an increase in the number of vulnerabilities—

along with the increasing interest among people and organizations with bad intent—increases the likelihood that risks will become actual events due to both accident and malfeasance. Indeed, in an article for the National Academy of Engineering, Massoud Amin, Professor at the University of Minnesota and formerly of EPRI, states that “cyber systems are the ‘weakest link’ in the electricity system.”²⁷ It will take a determined cybersecurity-aware review of the design and implementation of grid components and operational processes to reduce the likelihood of attack and the scope of potential impact.

The challenges to maintaining cybersecurity of the electric grid come from several characteristics of the future grid:

- **New control systems and processes:** Control over large amounts of information generated from grid operations at the individual utility and even consumer level will require new control and management systems and processes.
- **Components:** The electric grid will be composed of components from multiple suppliers, with multiple interfaces and protocols, and relying on multiple standards.
- **Continuous transition:** The information and communications technologies (ICT) used in the grid will continue to change at a faster rate than utilities can change components in the grid, resulting in incompatibilities and security vulnerabilities between existing and new ICT.

These characteristics of the future grid make it especially difficult to develop plans for improved cybersecurity, although efforts have been made and many more are under way to assist industry with this task. The Homeland Security Act of 2002 gave the U.S. Department of Homeland Security (DHS) primary respon-

It will take a determined cybersecurity-aware review of the design and implementation of grid components and operational processes to reduce the likelihood of attack and the scope of potential impact.

sibility for developing a comprehensive national plan to secure critical infrastructure. In December 2003, Homeland Security Presidential Directive 7 designated 17 critical infrastructure sectors and named the DOE to lead protection and resilience-building activities in the energy sector, including electricity. DHS and DOE produced a plan for that sector, as part of the National Infrastructure Protection Plan, published in June 2006, and it has been updated since.²⁸

In 2006, a Roadmap to Secure Control Systems in the Energy Sector was prepared for the DOE and DHS, which have been collaborating on its implementation since 2007.^{iv, 29} In 2010, the National Broadband Plan recommended (and the FCC is following up on) creating a more far-reaching Cybersecurity Roadmap for communications.³⁰ That same year, the GAO issued a report on challenges to cybersecurity research and development.³¹ In 2011, the DOE announced a public–private collaboration including NIST and NERC to develop guidelines for cybersecurity risk management in the electric sector.³²

^{iv} The Energy Sector Control Systems Working Group, a public–private partnership that includes representatives from the DOE and DHS, is tasked with implementing the roadmap. See <http://www.controlsroadmap.net/workinggroup.shtml>. The 2011 update to the 2006 roadmap is now available at <http://www.controlsroadmap.net/pdfs/roadmap.pdf>.

In response to heightened Congressional concern with cybersecurity, the administration issued a legislative proposal in May 2011 that would make DHS responsible for working with industry to enhance the cybersecurity of all the nation's critical infrastructure.³³ Two months later, the Senate Energy Committee reported out S. 1342, a bill that would make DOE and FERC responsible for cybersecurity of the electric power system. (Similar legislation, H.R. 5026, had passed the House in June 2010.) While both proposals would designate a single responsible agency, the administration seems to have given more weight to DHS's broad expertise in cybersecurity and its multisector responsibility, while the Congress seems to have given more weight to DOE and FERC's specific knowledge of the electric power industry.

With rapidly expanding connectivity and rapidly evolving threats, making the grid invulnerable to cyber events is impossible, and improving resilience to attacks and reducing the impact of attacks are important.

With rapidly expanding connectivity and rapidly evolving threats, making the grid invulnerable to cyber events is impossible, and improving resilience to attacks and reducing the impact of attacks are important. As a joint NERC–DOE report notes, “It is impossible to fully protect the system from every threat or threat actor. Sound management of these and all risks to the sector must take a holistic approach, with specific focus on determining the appropriate balance of resilience, restoration, and protection.”³⁴ For the electric grid in particular, cybersecurity must encompass not only the protection of information but also the security of grid equipment that depends on or is controlled by that information. And its goals must include ensuring the continuous and reliable operation of the electric grid.

The scale of investment required to improve cybersecurity is not insignificant. A 2011 EPRI report estimated that a \$3.7 billion investment is needed for grid cybersecurity, although this amount is relatively low compared to its estimate of a net total investment over 20 years of between \$338 and \$476 billion needed to realize the benefits of the smart grid.³⁵ But as GAO points out in a 2007 report, it is difficult to make the business case for investing in critical infrastructure cybersecurity because the probability of a serious event is still very low and the consequences are so difficult to quantify.³⁶ In a more recent report of 2011, the GAO finds a remedy in cybersecurity metrics for helping utilities show a return on a particular cybersecurity investment. “Until such metrics are developed,” the GAO concludes, “there is increased risk that utilities will not invest in security in a cost-effective manner, or have the information needed to make informed decisions on their cybersecurity investment.”³⁷ The National Science and Technology Council, reporting to the White House, also recognizes the importance of cost-effectiveness: “The [current] Administration’s approach to a secure grid is to pursue a thoughtful, cost-effective strategy that ensures the largest improvement in security and the greatest return on investment.”³⁸ Unfortunately, finding the approach that balances risk, impact, and cost will be a challenge for industry and government alike.

System Security and Designing for the Security Life Cycle

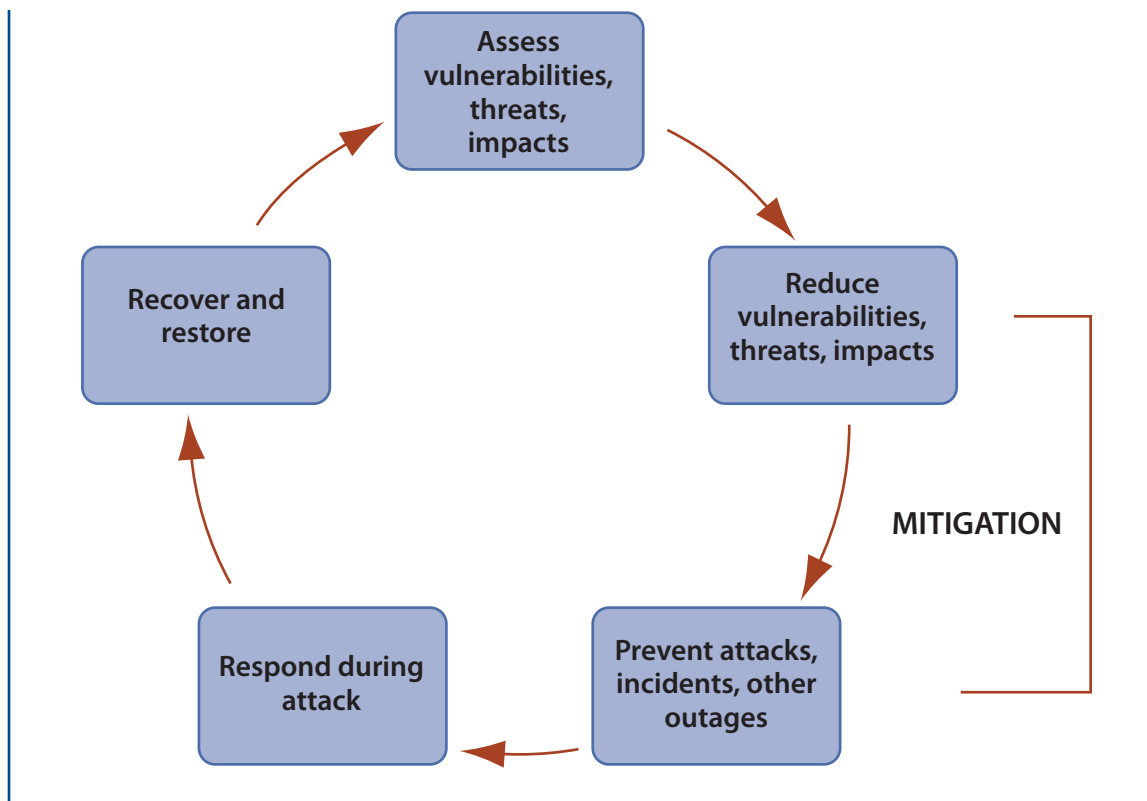
System security focuses on the holistic protection of systems and the prevention of attacks, beginning with system design and including the implementation of physical and electronic barriers, and activities to identify potential attackers. Figure 9.3 illustrates a multistep life-cycle approach to systems security that can be applied to analyzing cybersecurity of the electric grid.

The first step is to assess vulnerabilities, possible attack vectors, and the potential impact of attacks. NIST, overseeing a large public–private working group, published Guidelines for Smart Grid Cyber Security in 2010 to address these issues.³⁹ Risk mitigation, which focuses on reducing system vulnerabilities as well as preventing attack, should follow. Utilities, their suppliers, and government agencies all have a role to play: utilities are responsible for overall secure system design, operations, and control; suppliers ensure their equipment is designed for security; and government agencies carry out risk assessment, testing, certification, standards setting and regulation. Mitigation involves both reducing vulnerability and preventing attack, as the NERC–DOE High-impact, Low-frequency Event Risk report notes: “Perhaps the first step to adequate mitigation is the acknowledgment that fully protecting the system from a coordinated attack is not possible...As a result, effectively mitigating the

effects of a coordinated attack on the system will require a strong mix of preventative measures designed to build on the inherent resilience of the system and preparatory measures that will enable system operators to recognize an attack and respond to it when it does occur.”⁴⁰ Systems should all be designed to respond to attacks—for example, by ejecting attackers from the system or containing a problem to a localized area. In the case of the grid, one such tactic is to isolate circuits to minimize outages. Finally, systems should recover from the effects of an attack by restoring operations and retrieving or repairing corrupted data.

As the grid evolves, vulnerabilities and attack types will change quickly just as modern computer viruses do. Anticipating the possible impacts of attacks and focusing on resilient and robust responses can mitigate the negative effects more efficiently than attempting to

Figure 9.3 Security Life Cycle



defend against every new type of attack.⁴¹ We believe the natural evolution of grid information technologies already points toward such an approach: the development and integration of increasingly rapid and accurate systems control and monitoring technologies should facilitate quicker attack detection—and consequently, shorter response and recovery times. Cyber-attack response and recovery measures would be a fruitful area for ongoing research and development in utilities, their vendors, and academia.

FINDING

As communications systems expand into every facet of grid control and operations, their complexity and continuous evolution will preclude perfect protection from cyberattacks. Response and recovery, as well as protection, are important concerns for cybersecurity processes and regulation. Research funding will be important to the development of best practices for response to and recovery from cyberattacks.

Much as cybersecurity was not a key factor in the design of the Internet, cybersecurity has not been a high priority—until recently—in designing grid components. This can result in highly disturbing or even disastrous situations: consider the emergency shutdown of a nuclear power plant in Georgia after a software update on one system reset an important database on another when the two systems were linked.⁴² The Aurora experiment and the Stuxnet worm are two additional examples discussed later in this chapter. Experience from other domains shows that the most effective security is “designed in” and requires consideration of all aspects of the security life cycle.

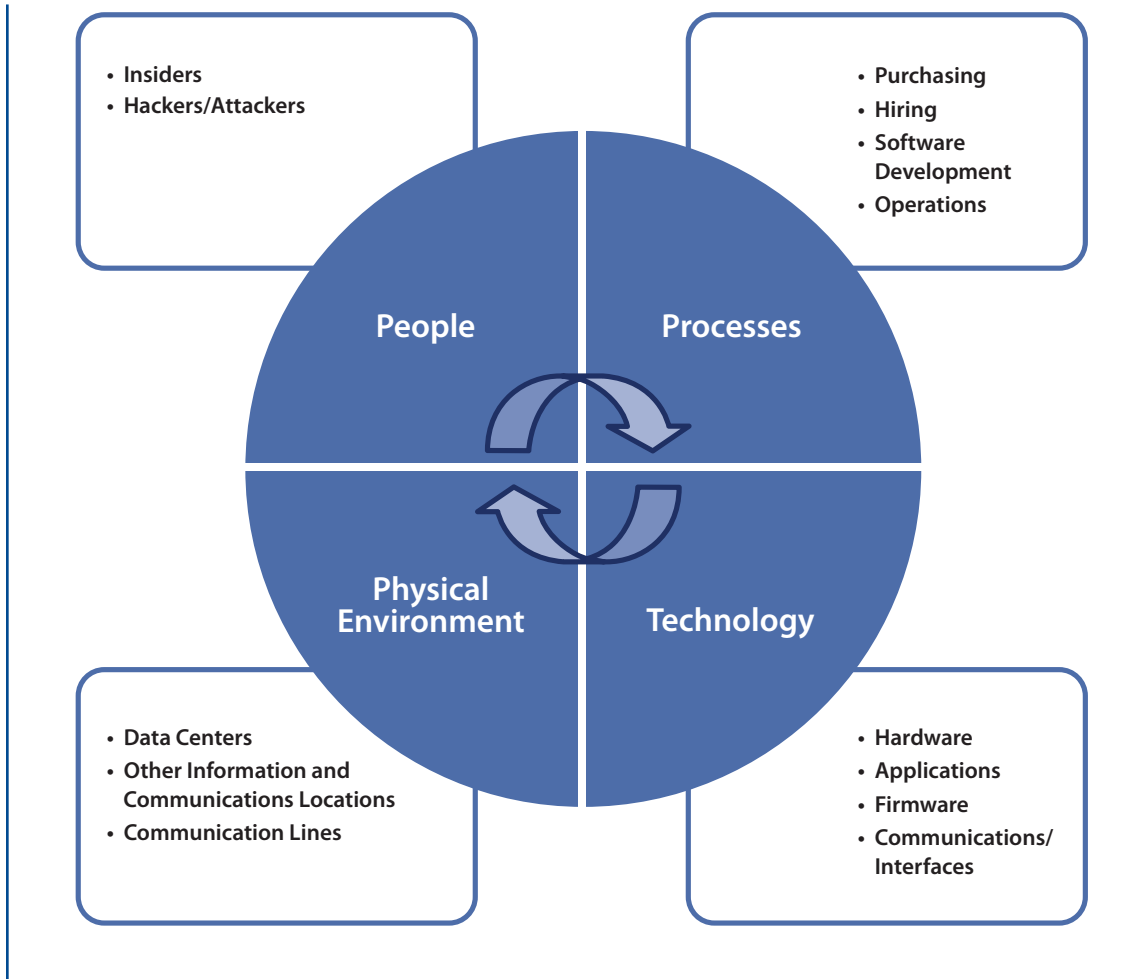
Vulnerabilities

Although effective attack responses will become important for the continued operation of the grid, the mitigation of grid cybersecurity vulnerabilities remains critical and is a responsibility of manufacturers, utilities, and the government. Achieving this task will increasingly require the electric sector to protect its IT and telecommunications infrastructure.⁴³ As the grid modernizes, the growing prevalence of information and communications technology in the system and the large numbers of personnel with access to it will create an ever-evolving cybersecurity situation, where the relative importance of specific vulnerabilities changes continuously as new types of attacks emerge. In particular, the introduction of the Internet to grid operations has introduced additional vulnerabilities to the power system, especially where corresponding security controls have not been put in place.⁴⁴

Cybersecurity vulnerabilities can arise from weaknesses in personnel, processes, technology, and the physical environment. Figure 9.4 shows examples in these categories.

Security issues occur because of actions taken by outside hackers and attackers, and also by disgruntled employees. With their insider knowledge, these individuals may instigate significant damage; for example, in 2000, an insider attack on the Australian water system caused the spillage of 800,000 liters of sewage into rivers and parks in Queensland.⁴⁵ A 2005 study by Robert Turk at the U.S. Computer Emergency Readiness Team’s Control Systems Security Center found that insiders perpetrated 38% of control system cybersecurity incidents.⁴⁶ More recently, DHS has issued a warning to utilities that “insiders and their actions pose a significant threat to the infrastructure and information systems of U.S. utilities.”⁴⁷

Figure 9.4 Categories of Cybersecurity Vulnerabilities



Process security ensures that all operational processes include measures to protect the enterprise, its equipment, and its products. In the case of grid cybersecurity, examples include running or validating the results of various security checks on equipment before certifying them for purchase, performing outside security checks on potential IT and communications hires, implementing software development processes that include security checklists, and doing physical security checks of computer and communications equipment areas.

Technology security involves the design, implementation, and interoperability of communications and IT hardware, application software, device-embedded software (“firmware” typically provided by the manufacturer),

communication protocols, and communications interfaces. The future grid also will have millions of programmable devices—most notably smart meters, but also electric vehicles, PMUs, devices in electric grid substations, and other equipment—that all present software application and firmware security vulnerabilities.

Communications security includes mitigating protocol vulnerabilities that can impact the ability of communications network protocols to transmit their data securely. In this case, some security issues and solutions may be dependent on the protocol in use. Communications interfaces within and between grid systems introduce critical vulnerability points into the electric grid network. For example, customer demand response might involve an

interface between AMI, distribution management systems, and billing systems spanning a large number of customers, with potentially multiple types and versions of communications components, even within a single utility's environment. Not only will such a system incur additional interoperability costs, but the additional complexity increases vulnerability to data tampering and other security issues. In its 2010 guidelines, NIST discusses such cybersecurity "use cases" and vulnerability classes in detail.⁴⁸

Control over physical access to grid hardware and facilities is also necessary to eliminate tampering at software and communications interfaces. Gaining physical access to a communications router or controller would allow a knowledgeable person to significantly disrupt data flow. Likewise, gaining access to a corporate data center or other equipment location would allow direct control over equipment.

Ultimately, utilities will have to consider what cybersecurity protections should be used in each new technology and system they implement. Examining real-world cases of how components and technologies are used in the grid will be just as important as considering individual components and their place in the total system environment. To demonstrate the multifaceted security risks that individual grid technologies face, Table 9.3 charts some attack vectors, possible impacts, and potential solutions related to one technology, AMI.^v

Component and Systems Testing

Rigorous testing of individual system components, complemented by integrated systems testing, can help mitigate cybersecurity risks and develop better system responses when vulnerabilities are breached. Several utilities

and industry stakeholders, including the Edison Electric Institute (EEI) and NERC, support federally sponsored system testing because of the government's technical expertise in the area of cybersecurity.⁴⁹

One notable government effort under way is the National SCADA (supervisory control and data acquisition) Test Bed program set up by DOE and operated by the Idaho National Laboratory, Sandia National Laboratory, and other partners. In this voluntary program, the lab conducts vulnerability assessments for control systems and third-party vendor equipment. Testing there has effectively revealed previously unknown vulnerabilities in control systems. For example, the "Aurora" experiment in 2007 discovered a severe weakness that would have enabled hacking into electric power control systems with potentially disastrous results.⁵⁰ After NERC's initial advisory shortly after this discovery, three years passed before it recommended mitigating strategies to the industry, with requirements for progress reports from covered utilities every six months.⁵¹

More rigorous procedures with regard to security testing might have reduced damage caused by the highly publicized Stuxnet worm, which was discovered in 2010 to have entered control systems using a common default password in certain SCADA equipment from Siemens.⁵² As early as September 2006, the Idaho National Laboratory had warned of the threat posed by weak passwords.⁵³ But because the National SCADA Test Bed procedures are voluntary and partner organizations sign nondisclosure agreements about work done there, it is unclear whether the Siemens system had undergone such testing or, if it had, whether the recommendations had been put into practice.

^v Case studies on the cybersecurity risks associated with not just AMI but also distribution grid management and electric vehicles are available from the Advanced Security Acceleration Project for the Smart Grid, a collaborative funded by DOE and various utility companies to accelerate the development of security requirements for the grid. See <http://www.smartgridipedia.org/index.php/ASAP-SG>.

Table 9.3 Attacks on Advanced Metering Infrastructure, with Possible Impacts and Solutions

Attack Vector	Impact	Possible Solutions	Solution Requirements
Physical Attack on Meter	Energy theft Incorrect energy usage data sent Theft of energy-usage data Theft of personal/billing information Disruption of electricity supply	Tamper-proof sealing or physical locks ^a Tamper-detection mechanisms ^b Automated system protection ^c (e.g., data erasure) Regular updates of meter firmware, security certificates ^d Asymmetric encryption ^d Frequent but irregular change of cryptographic keys, pre-installation of keys ^e Design architecture to store data for minimum time necessary ^b	Sufficient network bandwidth for updates ^d Formal industry agreement on a “sufficient” bandwidth Minimum security standards (regularly updated) regarding software security, tamper-proof and tamper-detection mechanisms Policy requirement for regular software updates to meet security standards Policy requirement for automated system protection
Denial-of-Service Attack on Meter Data Collection Point	Denial of service to connected local area meters, disruption of local-area network Possible upstream cascading effects on utility data network due to missing data	Tamper-detection mechanisms at collection points Automated system protection ^c (e.g., data erasure)	Standards for tamper-detection mechanisms
Software Attack on Utility Meter Data Management System	Widespread theft of energy-usage data Widespread theft of personal/billing information Disruption of electricity supply Disconnection of meters	Utility security policies to prevent unauthorized access Detection methods for unauthorized access/tampering Separation of electricity delivery system from energy data management system	Corporate security policies User access policies Back-end system design policies Implementation of utility-side tamper-detection mechanisms

Sources:

^aS. McLaughlin, D. Podkuiko, and P. McDaniel, “Energy Theft in the Advanced Metering Infrastructure,” in *Proceedings of the 4th International Workshop on Critical Information Infrastructure Security* (New York, NY: IEEE Press, 2009).

^bR. Shein, “Security Measures for Advanced Metering Infrastructure Components,” in *2010 Asia-Pacific Power and Energy Engineering Conference* (New York, NY: APPEEC and IEEE, 2010).

^cInGuardians, *Advanced Metering Infrastructure Attack Methodology, Vol 1.0*. (Washington, DC, 2009).

^dF. M. Cleveland, “Cyber Security Issues for Advanced Metering Infrastructure (AMI),” presented at the IEEE Power and Energy Society General Meeting, Pittsburgh, PA, July 20–24, 2008.

^eC. Bennett and D. Highfill, “Networking AMI Smart Meters,” presented at Energy 2030: IEEE Conference on Sustainable Energy Infrastructure, Atlanta, GA, November 17–18, 2008.

Assessments of system-level security also can help ensure appropriate security levels are maintained. In 2008, GAO undertook an extensive audit of control-system security in the largest U.S. public power company—the Tennessee Valley Authority. While it had begun several processes to improve cybersecurity prior to the GAO audit, management subsequently centralized cybersecurity responsibility so that cybersecurity and risk management policies would be more consistently applied to its control systems, and engaged a third-party to test for cybersecurity vulnerabilities.⁵⁴

Owing to rapid changes in cybersecurity risk as grid technologies develop, a system's level of security can change over time. Furthermore, the complex and quickly evolving technologies, systems, and security policies of the modernizing grid make it difficult to issue generic security design guidelines that remain appropriate over time. These factors reinforce the importance of ongoing component and systems testing.

Continuous Technology Transition

Some policy makers and state utility commissions are already concerned by the fast evolution of smart grid technologies and communications solutions. Indeed, a recent proposal by Baltimore Gas & Electric to deploy 1.36 million smart meters in Maryland was initially rejected by the Maryland PUC because of the high risk that meter technology will become obsolete, among other reasons. This will be the case if meters are installed without communications flexibility and/or the protocol they use is abandoned later on in the grid development process.⁵⁵ Looking even further ahead, EEI remarks, “Smart Grid technology itself may have a substantially shorter life-cycle than the equipment it replaced.”⁵⁶

Continuous transition also raises important cybersecurity issues. A specific security challenge is the problem posed by the smart meters that

have already been installed. An estimated 20 million AMI meters have been deployed nationwide as of June 2011.⁵⁷ The security features of these meters may be deemed inadequate under future cybersecurity standards, and the earliest smart meters may have been developed without taking into account the NIST Guidelines for Smart Grid Cyber Security released in 2010 or the AMI Security Profile developed by the Advanced Security Acceleration Project for the Smart Grid (see note v).⁵⁸

Utilities have stated that it is often necessary to continue using legacy equipment at least while new equipment is being installed and that it can be difficult to justify installing new equipment solely for security reasons.⁵⁹ One method of addressing the issues posed by systematic upgrade processes has been to insert a “shield,” or encapsulating device, between new and old grid components. The shield protects the devices below it from modern cyberattacks while the lower-level devices are being upgraded more slowly. The power technology firm ABB explains that such methods “encapsulate the given system within a secure zone of cyber protection so that it is isolated from direct contact with other systems, both within the utility firewall and outside it. Communication channels can also be secured by upgrading to modern protocols that support encryption, authentication and authorization mechanisms. Access to the legacy system can also be controlled by bolting on a new user interface layer along with the application of appropriate procedures for authorization.”⁶⁰

While continuous transition may pose cybersecurity risks to the grid, it may also present solutions. An industry observer has remarked that regulations encouraging continuous innovation in cybersecurity approaches can help ensure they remain able to meet the evolving threats to the grid.⁶¹ It is also worth noting that innovation in cybersecurity technologies and strategies could be limited by uncertainties over future regulation for

cybersecurity requirements, which would in turn hinder the development of a robust and resilient grid infrastructure.

Regulating Cybersecurity

Cybersecurity activities span all aspects of grid development and operations, from generation to transmission to distribution, and all aspects of risk management, from preparedness to prevention to response and recovery.

Regulation of these activities is in the hands of multiple regulatory and legislative bodies or, in some cases, of no such body (e.g., for cooperative or municipal utilities).

The principal regulations regarding grid cybersecurity are the NERC Critical Infrastructure Protection (CIP) standards, which apply to the U.S. bulk power system. They require responsible entities in this industry to submit documentation that identifies critical assets—as defined by specific criteria—and verify their cybersecurity preparedness.⁶² Noncompliance results in fines of up to \$1 million per day, although no fines approaching that amount have been levied to date.

One question about the current CIP standards is whether they focus industry too much on reporting and documentation rather than substantial cybersecurity improvements. CIP standards have been through multiple revisions with each aimed at helping to sharpening this focus toward improved cybersecurity. On a positive note, in 2010 an Arizona utility was able to detect and respond to a software virus attack with the help of systems originally installed to ensure CIP compliance.⁶³ On the other hand, a grid-system vendor reported that a utility met CIP requirements by decreasing the

level of sophistication in its network—ironically making the system less able to detect and respond to attacks.⁶⁴ In addition, a 2011 audit by the DOE Inspector General criticized FERC for approving CIP standards that did not contain commonly used security practices and adopted a poor approach to implementation.⁶⁵ Further modifications of the CIP standards are in progress.

The NIST Guidelines for Smart Grid Cyber Security go into greater depth on technical requirements, identifying different communications interfaces that exist or are expected to exist in the grid and technologies to secure them.⁶⁶ Unlike the CIP standards, which are more process-oriented and focus on the bulk power system, NIST's work is technical in nature and covers both the transmission and distribution domains.^{vi} As noted here, NIST also is working to facilitate the adoption by industry of appropriate national and international standards for the grid. Given the differences in focus and scope between the CIP and these standards, it appears unlikely that they would overlap substantially. However, the very presence of the two processes may confound stakeholders subject to both.^{vii}

One question about the current CIP standards is whether they focus industry too much on reporting and documentation rather than substantial cybersecurity improvements.

Apart from NERC's CIP standards, recommendations from NIST, and some nascent state PUC rulings (which do not cover municipal and cooperative electric distribution companies), there are no laws, regulations, or formal minimum standards for grid cybersecurity.

^{vi} A 2011 GAO report criticizes the NIST guidelines for their lack of information on combined cyber-physical attacks and the absence of a final schedule for updating the guidelines.⁶⁷

^{vii} The FCC identified the potential for conflicts between the existing CIP requirements and other standards as an area of concern and opined that the resulting ambiguity was slowing utility decision-making and deployment of some new technologies.⁶⁸

Furthermore, NERC's jurisdiction is limited to the bulk power system.⁶⁹ The distribution systems of investor-owned utilities, which account for approximately 66% of electricity sales, are regulated by individual state PUCs, while municipal and cooperative distribution utilities do not fall under any regulatory authority.⁷⁰ That said, given the level of technical specialization necessary to develop effective cybersecurity defenses and the need to continually update them, it would be inefficient for policy makers to dictate detailed technical cybersecurity specifications. Organizations such as the Institute of Electrical and Electronics Engineers and the International Electrochemical Commission already have extensive standards-setting processes which NIST has drawn on in its role as facilitator of grid standards. Instead, policy makers could focus their efforts on establishing security best-practice frameworks, as the NIST guidelines propose, to ensure that security regulations allow for rapid improvement and do not stifle innovation.

Compliance with standards does not necessarily make the grid secure.

Finally, it should be carefully noted that compliance with standards does not necessarily make the grid secure. EPRI explains, "Cybersecurity technologies and compliance with standards alone are not enough to achieve secure operations without policies, ongoing risk assessment, and training."⁷¹ Federal and state regulators are developing best-practice frameworks and model processes for response to and recovery from cyberattacks, based on a risk management approach, to help improve secure operations across the electric sector. For example, DOE, NIST, NERC and industry representatives are collaborating to develop an Electricity Sector Cybersecurity Risk Management Process Guideline, in draft form as of September 2011.⁷² These important

activities are all part of a "culture of security" that the utility industry must adopt.

While the consequences of a successful attack on the bulk power system are potentially much greater than an attack at the distribution level, the boundary between transmission and distribution has become increasingly blurry, and distribution-level cybersecurity risks deserve serious attention. Detailed consideration of the rapidly expanding interconnections between different levels of the grid will be critical to future efforts to address grid cybersecurity issues. State public utility commissions (which are generally responsible only for investor-owned distribution systems), municipal electric systems, cooperatives, and other public systems generally lack the expertise necessary to deal with cybersecurity issues.

FINDING

There is currently no national authority for overall grid cybersecurity preparedness. FERC and NERC have authority over cybersecurity standards development and compliance for the bulk power system, but there is no national regulatory oversight of cybersecurity standards compliance for the distribution system.

Forensics

Cyberattacks and accidents inevitably will occur in a system as large and complex as the grid. Forensics work focuses on discovering the root of cyber problems when they do occur and could significantly assist organizations in improving system design. Sharing this type of information with relevant stakeholders across the utility industry will allow the development of improved procedures and systems that can help prevent problems from reoccurring.

In the transportation industry, the National Transportation Safety Board analyzes major transportation events to identify sources of failure and makes recommendations for improvements to relevant government agencies, such as the Federal Aviation Administration. An analogous agency would be valuable in developing U.S. grid cybersecurity forensics. Because of the many parties involved in grid cybersecurity, such an agency might direct suggestions to industry and other stakeholders as well as to the federal government. DOE awarded two grants in September 2010 related to the creation of the National Electric Sector Cyber Security Organization, a nonprofit, independent entity that will serve such a function and facilitate information sharing between normally competitive or secretive parties more generally.⁷³ The organization will not have any regulatory authority. NERC also operates the Electricity Sector Information Sharing and Analysis Center. It exists to communicate threat indications, vulnerabilities, and protective strategies to industry members, government partners, and Information Sharing and Analysis Centers that have been established for other critical infrastructures. Experience in other industries shows that initiatives like these will be important to improving the reliability of the future grid.

9.3 INFORMATION PRIVACY AND SECURITY

Related to cybersecurity is the issue of information privacy and security. The future electric grid will collect, communicate, and store detailed operational data from tens of thousands of sensors as well as electricity-usage data from millions of consumers. This section discusses the issues that arise from making these data available to people who need them and protecting them from those who do not. Key

questions that are being addressed by the industry and regulators include:

- What data are we concerned about?
- How do we determine who should access that data, when, and how?
- How do we ensure that data are appropriately controlled and protected?
- How do we balance privacy concerns with the business or societal benefit of making data available?

Since these types of questions have been widely discussed in regard to other industries and data, this report will not attempt to provide a general treatise on information privacy and security but will focus on issues specific to access, usage, and disclosure of data that will be produced by operation of the future electric grid.^{viii} The electric utility industry and various government agencies are already concerned with these issues; recent major efforts by DOE, FCC, and NIST have solicited industry comments.⁷⁴ Indeed, the issue of protecting data privacy is not a new one for utilities. A resolution of the National Association of Regulatory Utility Commissioners more than 10 years ago urged the adoption of general privacy principles related to the use of utility customer information.⁷⁵

Categories of Privacy and Security Concerns

Security and privacy issues are evident in both major types of grid data: operational data and electricity consumption data (or “consumer electric usage data,” CEUD, according to the DOE terminology).

^{viii} The study of information privacy deals with policy issues ranging from identification and collection to storage, access, and use of information. The study of information security deals with protecting information from unauthorized access and use as defined by information privacy rules or otherwise.

Grid operational data is data or information about electricity generation, transmission, and distribution components or systems not at the level of individual customers.^{ix} Grid schematics, equipment and control signal specifications,

While privacy discussions in the popular press focus on consumer electric usage data, control over grid operational information is arguably more important.

and operating procedures are grid operational data. Load analysis of electricity flows across a transmission line and output logs from an electric generator at a hydroelectric plant are grid operational data. Improper disclosure of these or other operational information may result in tangible, or objective, competitive or societal harm.

CEUD is data obtained from measuring the electric usage of individual consumers, both commercial and residential.^x Improper disclosure of consumer-level information, such as minute-by-minute electricity usage, may result in objective harm as well as subjective, or intangible, harm. Property theft and physical attack are examples of the former. There are also more subjective privacy concerns about the harm “in which the mere knowledge by a second or third party of one’s private information is experienced [as] an injury.”⁷⁶ Consumer anxiety over the installation of smart meters and wide-scale implementation of AMI arises from both types of concern, and both deserve important consideration.

Privacy and Security of Operational Data

While privacy discussions in the popular press focus on consumer electric usage data, control over grid operational information is arguably more important, certainly in terms of large-scale impact on grid operations. Improper disclosure of grid operational information—such as operational procedures, network topology, control signals, and load-analysis data—may result in objective security or competitive harms, up to and including use of this data to mount physical or cyberattacks on the grid, such as was demonstrated in the Stuxnet attacks and the Aurora experiment.

In the past, corporate interests dominated this discussion with the privacy concern that competitive information would be disclosed. However, in the current worldwide environment, the government is concerned with the protection of information from a security standpoint because enemies could use the information to determine grid vulnerabilities. The protection of grid operational information is being dealt with by NERC for the bulk power system^{xi} and PUCs for the distribution system. The protection of grid operational information is commonly treated as a “security” issue rather than a “privacy” issue. Regardless of terminology, grid operational data protection deserves important consideration in policy and regulation.

^{ix} While “information” and “data” are used somewhat interchangeably, they are related but different terms; information is processed data.

^x Utilities also deal with “personally identifiable information” (PII) in the normal course of their operations, as do all companies in consumer-facing businesses. PII is any data or information that identifies an individual person or organization. For example, name, address, and phone number taken together are considered PII. The privacy issues related to PII have been addressed in many forums and are not discussed further in this report.

^{xi} See, for example, NERC Regulation CIP-003-4, which specifies implementation of a “cyber security policy that represents management’s commitment and ability to secure its Critical Cyber Assets.”

As important as grid operational security is, improper CEUD disclosure often attracts more public attention because it has the potential to directly harm individuals. The remainder of this section will focus on the privacy issues related to CEUD.

Privacy and Security of Consumer Data

For decades, electricity meters were primarily a source of monthly measurements to be used in creating consumers' bills. Now, new smart meters can measure electricity usage multiple times each hour. As Figure 9.5 shows, these data flow across the electric grid communication network not only to utilities but potentially to suppliers of third-party services and government agencies (some of these flows may be of aggregated or summary data). Objective and subjective privacy concerns resulting from that data collection and use include identity theft; personal surveillance by law-enforcement agencies and others; energy-use surveillance by business competitors and third-party service suppliers; physical danger from criminals; and other misuse of data.⁷⁷ Note that these uses of CEUD have nothing to do with operation of the grid or providing ancillary services. For example, the *Columbus Dispatch* reported that an Ohio utility routinely responds to subpoenas for utility usage information in drug enforcement actions.⁷⁸ Information privacy concerns are not limited to one type of organization or one type of use. Corporations, governments, and criminals are all cited as potential users of CEUD for wide-ranging purposes that may or may not be considered proper or legitimate by individual or business consumers.

CEUD is collected on all consumers of electricity, and a disclosure by a major electric company could affect millions of people and businesses. When electric usage was only measured once a month, most people were not particularly concerned about whether that data was protected or how it was used. But with millions of smart meters now installed, and tens of millions more on the way, access to the electric usage data they will generate is of much greater concern. These data do have many legitimate uses, including some that might be of value to home or business owners. For instance, the data can alert consumers to a malfunctioning appliance or equipment that is drawing excessive amounts of electricity.

It can also facilitate demand response systems and general home and business energy management systems. However, because the potential exists for other, perhaps less desirable uses, there are opposing views within the industry and in government about collecting and protecting these data. The following list exemplifies some of the discussion points:

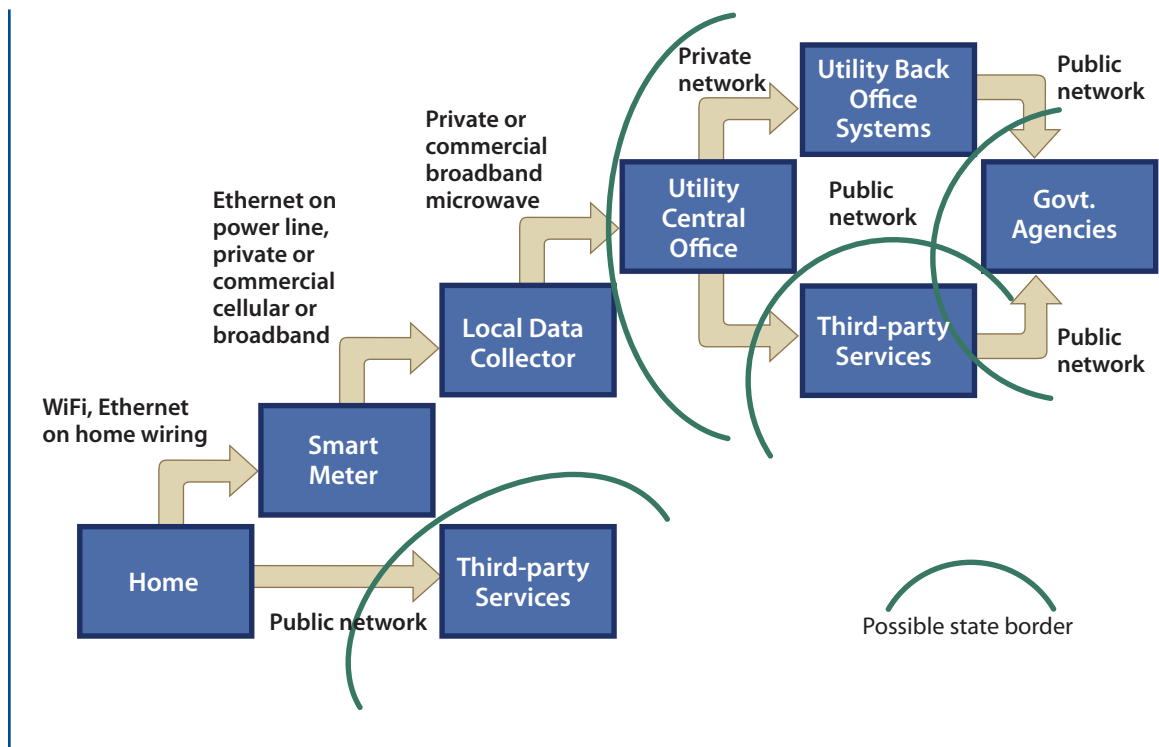
Information privacy concerns are not limited to one type of organization or one type of use.

- Data Collection

- *Point:* Collecting detailed electricity-usage information will provide many benefits through the introduction of new services and efficiencies.

- *Counterpoint:* Collecting detailed electricity-usage information (and making it available to consumers and third parties) opens a variety of data-disclosure issues and will incur significant costs to utilities, perhaps out of proportion to the benefits.

Figure 9.5 Consumer Electric Usage Data Flow



- Data Ownership
 - *Point*: Collected data is the property of the utilities, and these companies can determine what to do with it.
 - *Counterpoint*: CEUD is owned by the customer.
 - EEI expresses a third view: “The critical policy issue for Smart Grid development is not ownership of consumption data, but access to, usage and disclosure of that data.”⁷⁹
- Data Privacy
 - *Counterpoint*, as expressed by EEI: Utilities must update their policies and procedures to protect consumer data because smart grid technology “introduces new data collection and information sharing abilities related to customer energy usage, and raises significant privacy and data access issues.”⁸⁰
 - *Point*: Some consumers do not particularly care about keeping CEUD private.
 - *Counterpoint*: Other consumers do care. “A recent consumer survey conducted for EEI [indicates] that 46 percent of respondents believe it is ‘very important’ that their electricity usage be kept confidential, 29 percent believe it is ‘somewhat important,’ and 79 percent believe only customers and utilities should have access to smart meter information.”⁸¹
- Data Integrity
 - *Point*: Utilities have always protected consumer data. Existing laws provide adequate protections.

We discuss these points further in the sections that follow.

Data Collection and Storage

Smart meters are capable of recording and transmitting electricity-usage information every few minutes. These and other measurement devices installed in homes and businesses will become even more capable in the future, potentially achieving almost continuous monitoring of the electric usage of HVAC units, lighting systems, or other electric appliances. The policy issues these technological advances raise include questions about what data should be collected, why and by whom, how collection and storage should be paid for, who controls such data, and how it should be protected.

Potential suppliers of new types of energy services advocate data collection and storage where they think it will enhance their future business. This often puts utilities in a position to collect data that perhaps will be of more value to other businesses and consumers than it will be to them, a situation that creates a potential regulatory concern when it comes to paying for the data collection and storage. Google, for example, has made the case to the California PUC that utilities should provide real-time electricity usage information to consumers, noting that the mere installation of a smart meter “does not automatically mean that consumers will receive” this information.⁸² The Texas PUC engaged the utilities in forming a consortium that pays an outsourced vendor to provide a data repository and create a website for customer use.⁸³ In

Ontario, the provincial government is creating a “meter-data management repository” to store CEUD and make it available for consumers.⁸⁴ In this effort, government is taking on a role where commercial interests may be too disjointed or at odds with one another.

It is also important to consider whether data should be collected when we have little immediate use for it. Collecting and storing large amounts of data costs money and poses the inherent privacy risk of inadvertent, or even malicious, disclosure. In the financial industry, the increasing number of disclosures has spawned new laws and regulations, such as the Fair Credit Reporting Act and the Payment Card Industry Data Security Standards.^{xii} The surest way to limit these risks is to collect only the minimal amount of data needed for known purposes, an approach advocated by some with regard to the future electric grid, and embodied in the oft-cited privacy guidelines published by the Organisation for Economic Co-operation and Development.^{xiii, 85} However, this approach ignores the role of data collection in advancing the evolution of the electric grid. Given the relative immaturity of new grid technologies, demand response strategies, variable pricing policies, and the expected development of even more new capabilities that will enhance the efficiency of the grid, it would appear too limiting to mandate that all data collection has to have a currently acknowledged purpose. The California PUC, for example, is requiring that utilities disclose the purpose for collecting each type of data as part of their Smart Grid Deployment Plan, although how they will

^{xii} The Federal Trade Commission enforces the Fair Credit Reporting Act (see <http://www.ftc.gov/os/statutes/031224fcra.pdf>), which includes the ability of consumers to sue for damages if data are improperly disclosed by a credit reporting agency. The Payment Card Industry Security Standards Council was formed by major credit card companies to develop standards in an effort to reduce public disclosure of credit card information (see <https://www.pcisecuritystandards.org/index.shtml>).

^{xiii} As will be discussed in this chapter, there are several such guidelines from major national and international organizations. This particular stricture does not appear in the Fair Information Practice Principles published by the Federal Trade Commission and is often recommended for adoption related to regulation of the future grid.

analyze or approve such plans is not part of the rulemaking.⁸⁶ An appropriate function of the regulatory process is to balance the value of data collection with other concerns. In the utility industry, that regulatory process is still in its early stages.

measurement of electricity usage may tell them that? If not, then access, disclosure, or use of that type of information (which will certainly be available in the future, if not already) requires some type of regulation.

The DOE analysis of industry and consumer group responses showed that while consumer-advocacy groups strongly supported customers' rights to control access to CEUD, utility respondents had a variety of views. Nonetheless, DOE concluded that "consumers should have some protection that utilities will not disclose CEUD to third parties unless given affirmative consent, that third parties should also be required to protect the privacy and security of CEUD they receive, [and] that various controls should be put in place."⁸⁸ This conclusion did not attempt to resolve the issue of ownership (which will vary across states) but rather focused directly on regulation of access, use, and disclosure. DOE also did not address the costs of implementing processes to deal with "affirmative consent," privacy, and other controls, nor did it address the potential concern of data use within the utility itself for marketing or other non-operational purposes.

Congress also is beginning to acknowledge the importance of laws governing CEUD data disclosure, although legislation has not yet been passed. For example, HR 4860, 2010's Electric Consumer Right to Know Act, died in committee but attempted to address these issues head-on, directing FERC to issue guidelines for minimum privacy standards.⁸⁹

The important conclusion to draw from these various public and governmental discussions is that electricity customers will demand, and should have, significant control over access to data about their electricity usage, both to supply third-party services they consider valuable and to restrict other usage that they consider detrimental. The industry will need guidance via regulation on how to implement such customer control, and those regulations should

An appropriate function of the regulatory process is to balance the value of data collection with other concerns.

Data Access, Use, and Disclosure

Information privacy ensures that owners of data have control over who can access and use those data. As a result, ownership, access, use, and disclosure of CEUD are linked issues requiring careful analysis. Indeed, in an analysis of industry and consumer group responses to its request for information about smart grid data access, third-party use, and privacy, DOE found that "a significant number of commenters believed that the issue of access was more critical to a discussion of Smart Grid privacy issues than the issue of data ownership."⁸⁷

Electricity consumers can install measurement devices in their homes or businesses or on their appliances and other equipment and provide the data they collect to whomever they choose. However, less clear is the issue of ownership rights as it relates to data collected by electric utilities through smart meters or other devices owned by the utility. Utilities must have the ability to measure how much of their product

Electricity customers will demand, and should have, significant control over access to data about their electricity usage, both to supply third-party services they consider valuable and to restrict other usage that they consider detrimental.

they are supplying and to use that information to ensure the proper functioning of the grid and of their organizations. But do they have the right to know that a customer's TV was on for three hours on Tuesday evening if detailed

provide a consistent framework across the U.S. It is then up to the utilities to apply proper information security techniques to ensure that these controls are implemented.

Regulating Privacy of Consumer Data

From a societal point of view, government has varying roles in providing protections to voluntary and involuntary business relationships. A relationship between a bank and its customers is voluntary, for example, and a customer could use evaluation of the bank's privacy policies and controls as a factor in choosing among competing banks. An electric utility customer, on the other hand, rarely has a choice of suppliers and thus is required to accept whatever policies that supplier discloses.^{xiv} This puts an added burden on regulators to ensure that electric companies exercise prudence in creating and implementing plans for collecting, storing, and protecting consumer information.

Various parties have recommended that the Federal Trade Commission's Fair Information Practice Principles guide the development of regulation.⁹⁰ Forming the basis of existing laws in such sectors as credit reporting, financial information, electronic communications, and health information, these principles cover the following major topics:

- **Notice/Awareness:** "Consumers should be given notice of an entity's information practices before any personal information is collected from them."

- **Choice/Consent:** Consumers should have "options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information—i.e., uses beyond those necessary to complete the contemplated transaction. Such secondary uses can be internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties."
- **Access/Participation:** A consumer should be able "to access data about him or herself—i.e., to view the data in an entity's files—and to contest that data's accuracy and completeness."
- **Integrity/Security:** "Data should be accurate and secure."
- **Enforcement/Redress:** "It is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them."⁹¹

Other organizations, such as the American Institute of Certified Public Accountants,⁹² the Canadian Standards Association,⁹³ and the Organisation for Economic Co-operation and Development⁹⁴ have created similar (but not identical) sets of principles that can provide additional guidance to the regulatory process.

One key question is who should regulate privacy of CEUD. DOE and FCC put this responsibility with individual states, but the circumstances of data generation and communication in the future grid may favor broader

^{xiv}Note that electricity supply restructuring does not resolve this issue. Electricity customers may be able to choose the "generator" of their electricity, but they almost always have to deal with a single distributor—the utility that brings the electricity into the home or business and sends them the bill. The one exception is large industrial customer that may deal with more than one distributor.

action.⁹⁵ For example, municipal and cooperative electric utilities do not fall under either federal or state PUC jurisdiction in this regard. And data transmission across state lines (as shown in Figure 9.5) may complicate jurisdiction even for investor-owned utilities that are regulated by one or more state PUCs and by FERC. CEUD generated in a home or business may be transmitted to computer data centers owned or contracted by utilities that are in different states than the original source of the data. Similarly, they may be transmitted to third parties or government agencies in different states, either by the utility or the consumer themselves. As computer services and technology continue to advance to “the cloud,”

Regulating fundamental privacy principles now will ensure that data collection and storage systems do not have to be redesigned in the future and will help minimize the privacy challenges that may obstruct future grid projects.

where these services are provided by national or even international corporations with data centers in multiple jurisdictions, the likelihood of data crossing governmental boundaries becomes almost a certainty. As a result, a patchwork of individual state laws and regulations may not be the most effective or appropriate way to develop privacy and usage rules.

Regulating fundamental privacy principles now will ensure that data collection and storage systems do not have to be redesigned in the future and will help minimize the privacy challenges that may obstruct future grid projects. State PUCs are currently addressing these issues, and the North American Energy Standards Board in conjunction with the National Association of Regulatory Utility Commissioners and a dozen other organizations is preparing model business practices incorporating an analysis by NIST and other groups based on Fair Information Practice Principles. Non-regulated utilities should be encouraged to adopt these practices as well.⁹⁶

FINDING

Maintaining appropriate control over electricity usage and related data is already and will remain an important issue with both residential and commercial consumers. Privacy concerns must be addressed to ensure the success of grid enhancement and expansion projects and the willingness of electricity consumers to be partners in these efforts.

Consumer Education

Studies, industry comments, and press reports alike show the need for ongoing consumer education about the impacts and benefits of future grid technologies, particularly in relation to metering and changes in billing practices. DOE makes the important statement that “consumer education and outreach to consumer advocates—some of whom still view advanced metering technologies with suspicion—will thus be critical components of efforts to promote the adoption of Smart Grid technologies.”⁹⁷ The public increasingly is indicating the importance it attaches to information privacy issues, and this concern must be taken into account in any educational activities.⁹⁸ There appears to be broad agreement among industry and advocacy groups with this principle (although not necessarily with the specifics), as the EEI expresses: “Customers must be educated to understand the new privacy exposures presented by Smart Grid and be empowered to take steps to protect their privacy.”⁹⁹

9.4 CONCLUSIONS AND RECOMMENDATIONS

Data communications and cybersecurity technologies evolve rapidly and have life cycles much shorter than those of other electric grid components. The millions of communicating grid components likely to exist in the future will lead to a need for continuous transition among different models and versions of hardware and software. As a result, interoperability among new and legacy technologies will be an enduring challenge.

Additionally, we note the all-important role that education about cybersecurity and privacy issues will play in the development of the future grid, to disseminate practical information and counter incorrect information about these complex areas. These activities should be a part of general education about impacts and implications of new technologies and policies related to the future grid.

As described in this chapter, the successful integration of advanced data communications into electric grid control and operations will depend on utilities incorporating these new technologies and the extent of interoperability among different data communications technologies. Interoperability can be achieved through standardizing on specific technologies or protocols. The key trade-off is between early standardization (which may limit innovation) and late standardization (which may delay adoption and lead to future interoperability problems).

In the short run, NIST's facilitation of recommended standards will encourage market entry and facilitate interoperability. The Energy Independence and Security Act of 2007 gives FERC a role in "adopting" standards recommended by NIST, but it is unclear what the "adoption" of standards would mean in practice. As GAO recently reported, FERC

currently does not have any way of monitoring industry compliance with standards it adopts through this process and, furthermore, only has authority over the bulk power system. Legislation may not be required but clarification would be helpful.

The fundamental question is how to ensure that innovation continues in and around the standardization process. The imposition of detailed federal standards beyond those that emerge from this process would not appear to be productive, although federal agencies, state PUCs, utilities, and consumer groups each have important roles to play as participants in the standard-setting process.

RECOMMENDATION

NIST and state PUCs should continue to work with industry's organic standardization processes to foster the adoption of interoperability standards. Toward this end, Congress should clarify FERC's role in adopting NIST-recommended standards as specified in the Energy Independence and Security Act of 2007 to ensure a smoothly functioning industry-government partnership.

Grid cybersecurity will require preparedness but also a heightened focus on detection, response, and recovery strategies, including strengthened testing and assessment processes. Assessments of electric grid systems conducted as part of industry or regulatory processes would provide added impetus for utility suppliers to ensure development of systems with sufficient concern for cybersecurity. As both cyberattacks and cybersecurity technologies evolve quickly, developing detailed cybersecurity standards will not entirely solve this problem. It is important to ensure that utilities, their suppliers, and third-party vendors all have a culture of consistent and continuous attention

to cybersecurity challenges, and that the industry cooperates to disseminate assessment results to advance general cybersecurity in the electric sector.

Cybersecurity regulations for bulk power systems already exist in the form of the NERC Critical Infrastructure Protection reliability standards, but their scope is limited to the bulk power system and does not include the distribution system. Further, municipal distribution utilities and cooperatives are outside of the current regulatory environment. Public-private partnerships, such as the NIST Cyber Security Working Group, have made efforts to more comprehensively address grid cybersecurity but do not have regulatory authority. This lack of a single operational entity with responsibility for grid cybersecurity preparedness as well as response and recovery creates a security vulnerability in a highly interconnected electric power system comprising generation, transmission, and distribution.

RECOMMENDATION

The federal government should designate a single agency to have responsibility for working with industry and to have appropriate regulatory authority to enhance cybersecurity preparedness, response, and recovery across the electric power sector, including bulk power and distribution systems.

As noted above, the administration has proposed that DHS be the lead agency because of its broad multisector cybersecurity responsibilities, while proposals in Congress have focused on DOE and FERC because of their sector-specific expertise. Each agency has its strengths, and we do not feel qualified to choose between them. Once a lead agency has been designated, it should take all necessary steps to ensure that it has appropriate expertise by working with relevant federal agencies, NERC, state PUCs, public power authorities, and such expert organizations as the Institute of Electrical and Electronics Engineers and EPRI.

Expanded data collection and communications capabilities in the grid will result in a significant expansion of data about the electric grid system itself and of users of electricity. Maintaining appropriate control over electricity usage data is already and will remain an important issue with both residential and commercial consumers. Key societal concerns about information security and information privacy relate to access to and protection of information about grid operational data as well as consumer electricity usage data.

Industry and federal agencies have recommended that states establish regulations concerning privacy of CEUD, and the states are responding. However, we find that coordination of policy across states is necessary to mitigate concerns of companies that operate in multiple jurisdictions and of their customers as data on both companies and their customers cross state boundaries. Regulating fundamental privacy principles now will ensure that data collection and storage systems do not have to be redesigned in future, and will help minimize the privacy challenges that may obstruct future grid projects. State PUCs are currently addressing these issues, and the National Association of Regulatory Utility Commissioners and a dozen other organizations are preparing model business practices incorporating an analysis by NIST and other groups based on Fair Information Practice Principles. Non-regulated utilities should be encouraged to adopt these practices as well.

RECOMMENDATION

PUCs, in partnership with appropriate federal agencies, utilities, and consumer organizations, should focus on coordinating their activities to establish consistent privacy policies and process standards relating to consumer energy usage data as well as other data of importance to the operation of the future electric grid.

REFERENCES

- ¹Idaho National Laboratory, *Study of Security Attributes of Smart Grid Systems—Current Cyber Security Issues*, prepared for the Office of Electricity Delivery and Energy Reliability under the Department of Energy Idaho Operations Office (Idaho Falls, ID, 2009).
- ²North American Electric Reliability Corporation, *Reliability Considerations from the Integration of Smart Grid* (Princeton, NJ, 2010).
- ³North American Electric Reliability Corporation and U.S. Department of Energy, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System* (Washington, DC, 2010), 37, <http://www.nerc.com/files/HILF.pdf>.
- ⁴L. Tsoukalas and R. Gao, “From Smart Grids to an Energy Internet: Assumptions, Architectures and Requirements,” paper presented at Third International Conference on Electric Utility Deregulation and Restructuring and Power Technologies, Nanjing, China, April 6–9, 2008, 94; E. Lightner and S. Director, “Evolution and Progress of Smart Grid Development at the Department of Energy,” presentation to FERC-National Association of Regulatory Utility Commissioners Smart Grid Collaborative Workshop, Washington, DC, July 23, 2008; Electric Power Research Institute, *Report to NIST on the Smart Grid Interoperability Standards Roadmap* (Palo Alto, CA, 2009), http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Report_to_NIST_August10_2.pdf; National Institute for Standards and Technology, *Guidelines for Smart Grid Cyber Security*, NISTIR 7628 (Washington, DC, 2010), http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf; and National Institute for Standards and Technology, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, special publication 1108 (Washington, DC, 2010), http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.
- ⁵“Smart Grid 101: The Smart Grid,” *Smart Grid News.com*, January 20, 2010, http://www.smartgridnews.com/artman/publish/Business_Smart_Grid_101_Resources/The-Smart-Grid-1766.html.
- ⁶National Energy Technology Laboratory, *Integrated Communications* (Pittsburgh, PA, 2007), http://www.netl.doe.gov/smartgrid/referenceshelf/whitepapers/Integrated%20Communications_Final_v2_0.pdf.
- ⁷*Ibid.*
- ⁸NIST, “NIST Finalizes Initial Set of Smart Grid Cybersecurity Guidelines,” September 2, 2010, http://www.nist.gov/public_affairs/releases/nist-finalizes-initial-set-of-smart-grid-cyber-security-guidelines.cfm.
- ⁹National Energy Technology Laboratory, see note 6 above.
- ¹⁰*NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*. see note 4 above.
- ¹¹National Institute of Standards and Technology, “PAP01: Role of IP in the Smart Grid,” August 25, 2011, <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP01InternetProfile>.
- ¹²U.S. Department of Energy, *Communications Requirements of Smart Grid Technologies* (Washington, DC, 2010), http://www.doe.gov/sites/prod/files/gcprod/documents/Smart_Grid_Communications_Requirements_Report_10-05-2010.pdf; and *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, see note 4 above.
- ¹³National Institute of Standards and Technology, “NIST-Identified Standards for Consideration by Regulators, Release 1.0,” October 6, 2010, http://www.nist.gov/public_affairs/releases/upload/ferc-letter-10-6-2010.pdf.
- ¹⁴Federal Energy Regulatory Commission, “Smart Grid Interoperability Standards,” Docket No. RM11-2-000, 136 FERC 61,039, July 19, 2011, <http://www.ferc.gov/EventCalendar/Files/20110719143912-RM11-2-000.pdf>.
- ¹⁵National Science and Technology Council, *A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future* (Washington, DC: Executive Office of the President, 2011), 29.
- ¹⁶Electric Power Research Institute, *Estimating the Costs and Benefits of the Smart Grid*, technical report 1022519 (Palo Alto, CA: March 2011), 2–5.
- ¹⁷U.S. Government Accountability Office, *Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to Be Addressed* (Washington, DC, 2011).
- ¹⁸American Electric Power, “Comments of the American Electric Power Company, Inc. to the Federal Communications Commission on NBP Public Notice #2” (2009).
- ¹⁹S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, “Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies,” *Control Systems Magazine, IEEE* 21, no. 6 (2001): 11–25.

- ²⁰Arcadian Network, “Comments to the Federal Communications Commission on NBP Public Notice #2” (2009); and AT&T, “Comments to the Federal Communications Commission on NBP Public Notice #2” (2009).
- ²¹Federal Communications Commission, *Connecting America: The National Broadband Plan* (Washington, DC, 2010), 251, <http://download.broadband.gov/plan/national-broadband-plan.pdf>.
- ²²Federal Communications Commission, see note 21 above, page 251.
- ²³U.S. Department of Energy, see note 12 above, pages 40, 53.
- ²⁴Federal Communications Commission, see note 21 above, page 252–153.
- ²⁵K. Fehrenbacher, “AEP Calls for Dedicated Wireless Spectrum for Smart Grid,” *GigaOM*, August 25, 2009; and Utilities Telecom Council, “Dedicated Spectrum for Utilities—Frequently Asked Questions,” <http://www.utc.org/utc/dedicated-spectrum-utilities-frequently-asked-questions>.
- ²⁶North American Electric Reliability Corporation, *2009 Long Term Reliability Assessment of the Bulk Power System* (Washington, DC, 2009), 6, http://www.nerc.com/files/2009_LTRA.pdf.
- ²⁷M. Amin, “Securing the Electricity Grid,” *The Bridge* 40, no. 1 (2010): 13.
- ²⁸U.S. Department of Energy and U.S. Department of Homeland Security, *Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan* (Washington, DC, 2010), <http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf>.
- ²⁹Energetics, *Roadmap to Secure Control Systems in the Energy Sector* (Columbia, Maryland, 2006), http://www.controlsystmsroadmap.net/pdfs/2006_roadmap.pdf.
- ³⁰Federal Communications Commission, “FCC Releases Agenda for Workshop on Cybersecurity Roadmap,” public notice, November 2, 2010; Federal Communications Commission, “FCC Seeks Public Comment on National Broadband Plan Recommendation to Create a Cybersecurity Roadmap,” public notice, August 9, 2010.
- ³¹U.S. Government Accountability Office, *Key Challenges Need to Be Addressed to Improve Research and Development* (Washington, DC, 2010).
- ³²U.S. Department of Energy, “The Department of Energy Launches Cyber Security Initiative,” press release, February 1, 2011, <http://energy.gov/oe/articles/department-energy-launches-cyber-security-initiative>.
- ³³The White House, “Cybersecurity Legislative Proposal,” fact sheet, May 12, 2011, <http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal>.
- ³⁴North American Electric Reliability Corporation and U.S. Department of Energy, see note 3 above.
- ³⁵Electric Power Research Institute (EPRI), note 16 above.
- ³⁶U.S. Government Accountability Office, *Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain* (Washington, DC, 2007), <http://www.gao.gov/products/GAO-07-1036>.
- ³⁷U.S. Government Accountability Office, see note 17 above.
- ³⁸National Science and Technology Council, see note 15, page 49.
- ³⁹NIST, see note 8 above.
- ⁴⁰North American Electric Reliability Corporation and U.S. Department of Energy, see note 3 above.
- ⁴¹North American Electric Reliability Corporation and U.S. Department of Energy, see note 3 above.
- ⁴²B. Krebs, “Cyber Incident Blamed for Nuclear Power Plant Shutdown,” *The Washington Post*, June 5, 2008, <http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html>.
- ⁴³Electric Power Research Institute, *Report to NIST on the Smart Grid Interoperability Standards Roadmap* (Palo Alto, CA, 2009).
- ⁴⁴Amin, see note 27 above, page 13.
- ⁴⁵M. Abrams and J. Weiss, “Malicious Control System Cyber Security Attack Case Study—Maroochy Water Services, Australia” (McLean, VA: The MITRE Corporation, 2008).
- ⁴⁶R. J. Turk, *Cyber Incidents Involving Control Systems*, INL/EXT-05-00671 (Idaho Falls, ID: Idaho National Laboratory, 2005), <http://www.inl.gov/technicalpublications/Documents/3480144.pdf>.
- ⁴⁷B. Ross, R. Schwartz, and M. Chuchmach, “New Terror Report Warns of Insider Threat to Utilities,” *ABCNews.com*, July 20, 2011, <http://abcnews.go.com/Blotter/terror-alert-warns-insider-threat-infrastructure/story?id=14118119>.
- ⁴⁸National Institute for Standards and Technology, *Guidelines for Smart Grid Cyber Security*, see note 4 above.

- ⁴⁹Edison Electric Institute, “Response of the Edison Electric Institute to the Department of Energy Request for Information on ‘Addressing Policy and Logistical Challenges to Smart Grid Implementation’” (2010), http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/EEI_-_DOE_SG_RFI.PDF; and North American Electric Reliability Corporation and U.S. Department of Energy, see note 3 above.
- ⁵⁰J. Meserve, “Staged Cyber Attack Reveals Vulnerability in Power Grid,” *CNN*, September 26, 2007, http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US.
- ⁵¹North American Electric Reliability Corporation, “NERC Issues AURORA Alert to Industry,” press release, October 14, 2010, http://www.nerc.com/fileUploads/File/PressReleases/PR_AURORA_14_Oct_10.pdf.
- ⁵²R. McMillan, “After Worm, Siemens Says Don’t Change Passwords,” *PC World*, July 19, 2010.
- ⁵³R. Fink, D. Spencer, and R. Wells, *Lessons Learned from Cyber Security Assessments of SCADA and Energy Management Systems* (Washington, DC: U.S. Department of Energy, 2006).
- ⁵⁴U.S. Government Accountability Office, *TVA Needs to Address Weaknesses in Control Systems and Networks*, Appendix II (Washington, DC, 2008).
- ⁵⁵Public Service Commission of Maryland Order No. 83410, In the Matter of the Application of Baltimore Gas & Electric to Deploy a Smart Grid Initiative and to Establish a Surcharge for the Recovery of Cost, June 22, 2010.
- ⁵⁶Edison Electric Institute, see note 49 above, page 60.
- ⁵⁷Federal Energy Regulatory Commission, *2011 Assessment of Demand Response and Advanced Metering Staff Report* (Washington, DC, 2011).
- ⁵⁸*Guidelines for Smart Grid Cyber Security*, see note 4 above; and Advanced Security Acceleration Project for the Smart Grid, *Security Profile for Advanced Metering Infrastructure*, Version 2.0 (2010), http://www.smartgridipedia.org/images/9/90/AMI_Security_Profile_-_v2_0.pdf.
- ⁵⁹Edison Electric Institute, note 49 above, page 54; American Public Power Association, “Comments of the American Public Power Association in the Matter of Addressing Policy and Logistical Challenges to Smart Grid Implementation,” (2010), 2.
- ⁶⁰ABB, Letter to Ms. Patricia Hoffman, Assistant Secretary, U.S. Department of Energy, November 2, 2010, 2, www.doe.gov/sites/prod/files/oeprod/DocumentsandMedia/ABB_Comments.pdf.
- ⁶¹Daniel Thanos, Chief Cybersecurity Architect, GE Digital Energy, personal communication with the authors, October 25, 2010.
- ⁶²North American Electric Reliability Corporation, “Project 2008-06: Cyber Security Order 706 Phase II,” January 24, 2011, http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html; North American Electric Reliability Corporation, Cyber Security—Critical Cyber Asset Identification, Standard CIP—002—4, adopted January 24, 2011; and North American Electric Reliability Corporation, Cyber Security—Critical Cyber Asset Identification, Standard CIP—002—3, adopted December 16, 2009.
- ⁶³E. Messmer, “Antivirus Software Didn’t Help in Zero-Day Malware Attack on Power Plant,” *Network World*, November 2, 2010, <http://www.networkworld.com/news/2010/110210-here-you-have-virus.html>.
- ⁶⁴See note 61 above.
- ⁶⁵U.S. Department of Energy Office of Inspector General, *Audit Report: Federal Energy Regulatory Commission’s Monitoring of Power Grid Cyber Security* (Washington, DC, 2011).
- ⁶⁶National Institute for Standards and Technology, *Guidelines for Smart Grid Cyber Security*, see note 4 above.
- ⁶⁷U.S. Government Accountability Office, see note 17 above.
- ⁶⁸Federal Communications Commission, see note 21 above.
- ⁶⁹D. Whiteley, *Testimony of David A. Whiteley, Executive Vice President, NERC before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology Committee on Homeland Security U.S. House of Representatives on “The Cyber Threat to Control Systems: Stronger Regulations are Necessary to Secure the Electric Grid,”* October 25, 2007.
- ⁷⁰U.S. Energy Information Administration, *Electric Sales, Revenue, and Average Price 2009* (Washington, DC: U.S. Department of Energy, 2010), Table 5A, http://www.eia.gov/cneaf/electricity/esr/table5_a.html.
- ⁷¹Electric Power Research Institute, see note 16 above, pages 2–5.

- ⁷²U.S. Department of Energy, “The Department of Energy Releases Draft of Cybersecurity Risk Management Process (RMP) Guideline for Public Comment,” press release, September 12, 2011, Washington, DC, <http://energy.gov/oe/articles/department-energy-releases-draft-cybersecurityrisk-management-process-rmp-guideline> (accessed September 13, 2011).
- ⁷³U.S. Department of Energy, “Secretary Chu Announces Latest Efforts to Address Cybersecurity,” press release, September 23, 2010, <http://energy.gov/articles/secretary-chu-announces-latest-efforts-address-cybersecurity>.
- ⁷⁴U.S. Department of Energy, *Data Access and Privacy Issues Related to Smart Grid Technologies* (Washington, DC, 2010), http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf; Federal Communications Commission, see note 21 above; and *Guidelines for Smart Grid Cyber Security*, see note 4 above.
- ⁷⁵National Association of Regulatory Utility Commissioners, *Resolution Urging the Adoption of General Privacy Principles for State Commission Use in Considering the Privacy Implications of the use of Utility Customer Information* (Washington, DC, 2000).
- ⁷⁶E. Dyson, “Reflections on Privacy 2.0.” *Scientific American* 299, 3 (September 2008): 50.
- ⁷⁷L. Coney, “Privacy Perspective on Protecting the Grid and Consumer Data,” presentation at the Smart Grid Summit, Washington, DC, April 8, 2010, http://epic.org/privacy/smartgrid/EPIC_Statement_Smart_Grid_Summit_Cybersecurity_and_Privacy.pdf.
- ⁷⁸D. Narciso, “Police Seek Utility Data for Homes of Marijuana-Growing Suspects,” *Columbus Dispatch*, February 28, 2011, http://www.dispatch.com/live/content/local_news/stories/2011/02/28/police-suspecting-home-pot-growing-get-power-use-data.html.
- ⁷⁹Edison Electric Institute, see note 49 above.
- ⁸⁰Edison Electric Institute, see note 49 above.
- ⁸¹Edison Electric Institute, see note 49 above.
- ⁸²Google, Inc., “Comments of Google Inc. on Proposed Policies and Findings Pertaining to the Smart Grid Policies Established by the Energy Information and Security Act of 2007” (2009), <http://www.google.com/powermeter/about/cpuc.html>.
- ⁸³“Smart Meter Texas”, <https://www.smartmetertexas.com/CAP/public/index.html>.
- ⁸⁴Ontario Ministry of Energy, “Smart Meters and Time of Use Pricing: FAQs,” http://www.mei.gov.on.ca/en/energy/conservation/smartmeters/?page=powersmarter_faqs#mdmr.
- ⁸⁵Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris, 1980), http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.
- ⁸⁶Public Utilities Commission of the State of California, “Decision Adopting Requirements for Smart Grid Deployment Plans,” rulemaking 08-12-009, June 28, 2010, http://docs.cpuc.ca.gov/PUBLISHED/FINAL_DECISION/119902.htm.
- ⁸⁷U.S. Department of Energy, see note 74, page 26.
- ⁸⁸U.S. Department of Energy, see note 74, pages 15–16.
- ⁸⁹Electric Consumer Right to Know Act, H.R. 4860, 111th Congress (2010), <http://www.govtrack.us/congress/bill.xpd?bill=h111-4860>.
- ⁹⁰See for example, J. Lynch and L. Tien, “Joint Comments of the Center for Democracy & Technology and the Electronic Frontier Foundation on Proposed Policies and Findings Pertaining to the Smart Grid,” March 9, 2010, <http://docs.cpuc.ca.gov/efile/CM/114696.pdf>.
- ⁹¹Federal Trade Commission, “Fair Information Practice Principles,” <http://www.ftc.gov/reports/privacy3/fairinfo.shtm>.
- ⁹²American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants Privacy Task Force, *Generally Accepted Privacy Principles* (New York NY: 2009), <http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/default.aspx>.
- ⁹³Canadian Standards Association Technical Committee on Privacy, *Model Code for the Protection of Personal Information*, CSA Standard CAN/CSA-Q830 (Mississauga, Ontario, 1996), <http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code>.
- ⁹⁴Organisation for Economic Co-operation and Development, see note 85 above.
- ⁹⁵U.S. Department of Energy, see note 74 above, page 15–16; and Federal Communications Commission, see note 21 above, page 256.

⁹⁶C. Wright, “NAESB Data Privacy Task Force Update,” presentation at the North American Energy Standards Board, Board of Directors meeting, March 24, 2011, <http://www.naesb.org/pdf4/bd032411w1.pdf>.

⁹⁷U.S. Department of Energy, see note 74 above, page 8.

⁹⁸Edison Electric Institute, *Public Opinion on Customers' Information Privacy* (Washington, DC, 2010).

⁹⁹Edison Electric Institute, see note 49 above, page 4.