United States Government Accountability Office

Testimony

Before the Subcommittees on Energy and Research and Technology, Committee on Science, Space, and Technology, House of Representatives

For Release on Delivery
Expected at 10 a.m. ET
Wednesday, October 21, 2015

CRITICAL INFRASTRUCTURE PROTECTION

Cybersecurity of the Nation's Electricity Grid Requires Continued Attention

Statement of Gregory C. Wilshusen,
Director, Information Security Issues

October 21, 2015

CRITICAL INFRASTRUCTURE PROTECTION

Cybersecurity of the Nation's Electricity Grid Requires Continued Attention

Highlights of GAO-16-174T, a testimony before the Subcommittees on Energy and Research and Technology, Committee on Science, Space, and Technology, House of Representatives

Why GAO Did This Study

The electric power industry—including transmission and distribution systems—increasingly uses information and communications technology systems to automate actions with the aim of improving the electric grid's reliability and efficiency. However, such "smart grid" technologies may be vulnerable to cyber-based attacks and other threats that could disrupt the nation's electricity infrastructure. Several federal entities have responsibilities for overseeing and helping to secure the electricity grid. Because of the proliferation of cyber threats, since 2003 GAO has designated protecting the systems supporting U.S. critical infrastructure (which includes the electricity grid) as a high-risk area.

GAO was asked to provide a statement on opportunities to improve cybersecurity for the electricity grid. In preparing this statement, GAO relied on previous work on efforts to address cybersecurity of the electric sector.

What GAO Recommends

In its 2011 report, GAO recommended that (1) NIST improve its cybersecurity standards, (2) FERC assess whether challenges identified by GAO should be addressed in ongoing cybersecurity efforts, and (3) FERC coordinate with other regulators to identify strategies for monitoring compliance with voluntary standards. The agencies agreed with the recommendations, but FERC has not taken steps to monitor compliance with voluntary standards.

View GAO-16-174T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

GAO reported in 2011 that several entities—the North American Electric Reliability Corporation (NERC), the National Institute of Standards and Technology (NIST), the Federal Energy Regulatory Commission (FERC), the Department of Homeland Security (DHS), and the Department of Energy (DOE)—had taken steps to help secure the electric grid. These included developing cybersecurity standards and other guidance to reduce risks.

While these were important efforts, GAO at that time also identified a number of challenges to securing the electricity grid against cyber threats:

- *Monitoring implementation of cybersecurity standards*: GAO found that FERC had not developed an approach, coordinated with other regulatory entities, to monitor the extent to which the electricity industry was following voluntary smart grid standards, including cybersecurity standards.
- *Clarifying regulatory responsibilities:* The nature of smart grid technology can blur traditional lines between the portions of the grid that are subject to federal or state regulation. In addition, regulators may be challenged in responding quickly to evolving cybersecurity threats.
- *Taking a comprehensive approach to cybersecurity:* Entities in the electricity industry (e.g., utilities) often focused on complying with regulations rather than taking a holistic and effective approach to cybersecurity.
- *Ensuring that smart grid systems have built-in security features:* Smart grid devices (e.g., meters) did not always have key security features such as the ability to record activity on systems or networks, which is important for detecting and analyzing attacks.
- *Effectively sharing cybersecurity information:* The electricity industry did not have a forum for effectively sharing information on cybersecurity vulnerabilities, incidents, threats, and best practices.
- *Establishing cybersecurity metrics:* The electricity industry lacked sufficient metrics for determining the extent to which investments in cybersecurity improved the security of smart grid systems.

Since 2011, additional efforts have been taken to improve cybersecurity in the sector. For example, in 2013, NERC issued updated standards to address these and other cybersecurity challenges. NIST also updated its smart grid cybersecurity standards in 2014. It has also developed a cybersecurity framework for critical infrastructure, and DHS and DOE have efforts under way to promote its adoption. In addition, FERC assessed whether these and other challenges should be addressed in its ongoing cybersecurity efforts. However, FERC did not coordinate with other regulators to identify strategies for monitoring compliance with voluntary cybersecurity standards in the industry, as GAO had recommended. As a result, FERC does not know the extent to which such standards have been adopted or whether they are effective. Given the increasing use of information and communications technology in the electricity subsector and the evolving nature of cyber threats, continued attention can help mitigate the risk these threats pose to the electricity grid.

Chairman Weber, Chairwoman Comstock, Ranking Members Grayson and Lipinski, and Members of the Subcommittees:

Thank you for inviting me to testify at today's hearing on efforts by federal agencies, including the Department of Energy, and industry to mitigate cybersecurity threats to U.S. power systems. As you know, the electric power industry is increasingly incorporating information and communications technologies (ICT) and networks into its existing infrastructure (e.g., electricity networks including power lines and customer meters). This use of ICT can provide many benefits, such as greater efficiency and lower costs to consumers. Along with these anticipated benefits, however, cybersecurity and industry experts have expressed concern that, if not implemented securely, modernized electricity grid systems will be vulnerable to attacks that could result in widespread loss of electrical services essential to maintaining our national economy and security.

Since 2003 we have identified protecting systems supporting our nation's critical infrastructure (which includes the electricity grid) as a high-risk area, and we continue to do so in the most recent update to our high-risk list.[1]

In my testimony today, I will describe actions taken and opportunities remaining to secure the grid against cyber attacks. In preparing this statement we relied on our previous work in this area, including studies examining efforts to secure the electricity grid and the associated challenges and cybersecurity guidance.[2] We also considered actions taken by agencies in implementing the recommendations from our prior report on cybersecurity of the electricity grid. The prior reports cited

[1]GAO's biennial high-risk list identifies government programs that have greater vulnerability to fraud, waste, abuse, and mismanagement or need transformation to address economy, efficiency, or effectiveness challenges. We have designated federal information security as a government-wide high-risk area since 1997, and in 2003 expanded this area to include computerized systems supporting the nation's critical infrastructure. Most recently, in the 2015 update to our high-risk list, we further expanded this area to include protecting the privacy of personally identifiable information (PII)—that is, personal information that is collected, maintained, and shared by both federal and nonfederal entities. See, most recently, GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

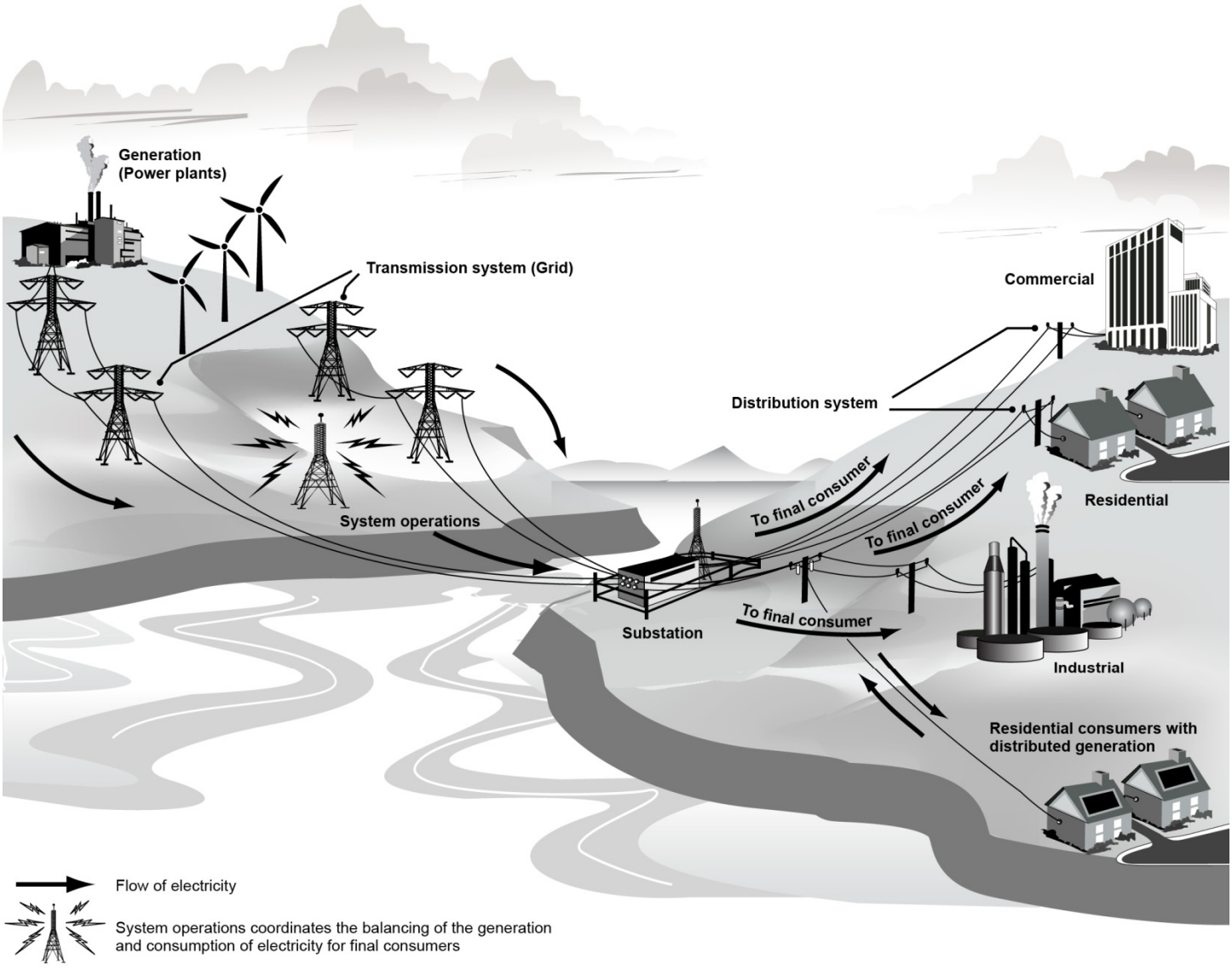
[2]GAO, *Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use*, GAO-12-92 (Washington, D.C.: Dec. 9, 2011), and *Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed*, GAO-11-117 (Washington, D.C.: Jan. 12, 2011).

throughout this statement contain detailed discussions of the scope of the work and the methodology used to develop each of them. All the work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The electricity industry, as shown in figure 1, is composed of four distinct functions: generation, transmission, distribution, and system operations. Once electricity is generated—whether by burning fossil fuels; through nuclear fission; or by harnessing wind, solar, geothermal, or hydro energy—it is generally sent through high-voltage, high-capacity transmission lines to local electricity distributors. Once there, electricity is transformed into a lower voltage and sent through local distribution lines for consumption by industrial plants, businesses, and residential consumers. Because electric energy is generated and consumed almost instantaneously, the operation of an electric power system requires that a system operator constantly balance the generation and consumption of power.

Figure 1: Functions of the Electricity Industry



Source: GAO. | GAO-16-174T

Utilities and others own and operate electricity assets, which may include generation plants, transmission lines, distribution lines, and substations—structures often seen in residential and commercial areas that contain technical equipment such as switches and transformers to ensure smooth, safe flow of current and regulate voltage. Utilities may be owned

by investors, municipalities, and individuals (as in cooperative utilities). System operators—sometimes affiliated with a particular utility or sometimes independent and responsible for multiple utility areas—manage the electricity flows. These system operators manage and control the generation, transmission, and distribution of electric power using control systems—IT- and network-based systems that monitor and control sensitive processes and physical functions, including opening and closing circuit breakers.[3]

As we have previously reported, the effective functioning of the electricity industry is highly dependent on these control systems.[4] Nevertheless, for many years, aspects of the electricity network lacked (1) technologies—such as sensors—to allow system operators to monitor how much electricity was flowing on distribution lines, (2) communications networks to further integrate parts of the electricity grid with control centers, and (3) computerized control devices to automate system management and recovery.

Modernization of the Electricity Infrastructure

As the electricity industry has matured and technology has advanced, utilities have begun taking steps to update the electricity grid—the transmission and distribution systems—by integrating new technologies and additional IT systems and networks. Though utilities have regularly taken such steps in the past, industry and government stakeholders have begun to articulate a broader, more integrated vision for transforming the electricity grid into one that is more reliable and efficient; facilitates alternative forms of generation, including renewable energy; and gives consumers real-time information about fluctuating energy costs.

This vision—the smart grid—would increase the use of IT systems and networks and two-way communication to automate actions that system operators formerly had to make manually. Electricity grid modernization is an ongoing process, and initiatives have commonly involved installing advanced metering infrastructure (smart meters) on homes and commercial buildings that enable two-way communication between the utility and customer. Other initiatives include adding “smart” components to provide the system operator with more detailed data on the conditions

[3]Circuit breakers are devices used to open or close electric circuits. If a transmission or distribution line is in trouble, a circuit breaker can disconnect it from the rest of the system.

[4]GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO-07-1036 (Washington, D.C.: Sept. 10, 2007).

of the transmission and distribution systems and better tools to observe the overall condition of the grid (referred to as “wide-area situational awareness”). These include advanced, smart switches on the distribution system to reroute electricity around a troubled line and high-resolution, time-synchronized monitors—called phasor measurement units—on the transmission system.

The use of smart grid systems may have a number of benefits, including improved reliability with fewer and shorter outages, downward pressure on electricity rates resulting from the ability to shift peak demand, an improved ability to more efficiently use alternative sources of energy, and an improved ability to detect and respond to potential attacks on the grid.

Regulation of the Electricity Industry

Both the federal government and state governments have authority for overseeing the electricity industry. For example, the Federal Energy Regulatory Commission (FERC) regulates rates for wholesale electricity sales and transmission of electricity in interstate commerce. This includes approving whether to allow utilities to recover the costs of investments they make to the transmission system, such as some smart grid investments. Meanwhile, local distribution and retail sales of electricity are generally subject to regulation by state public utility commissions.

State and federal authorities also play key roles in overseeing the reliability of the electric grid. State regulators generally have authority to oversee the reliability of the local distribution system. The North American Electric Reliability Corporation (NERC) is the federally designated U.S. Electric Reliability Organization, and is overseen by FERC. NERC has responsibility for conducting reliability assessments and developing and enforcing mandatory standards to ensure the reliability of the bulk power system—i.e., facilities and control systems necessary for operating the transmission network and certain generation facilities needed for reliability. NERC develops reliability standards collaboratively through a deliberative process involving utilities and others in the industry, which are then sent to FERC for approval. These standards include critical infrastructure protection standards for protecting electric utility-critical and cyber-critical assets. FERC has responsibility for reviewing and approving the reliability standards or directing NERC to modify them.

In addition, the Energy Independence and Security Act of 2007[5] established federal policy to support the modernization of the electricity

[5]Pub. L. No. 110-140 (Dec. 19, 2007).

grid and required actions by a number of federal agencies, including the National Institute of Standards and Technology (NIST), FERC, and the Department of Energy. With regard to cybersecurity, the act required NIST and FERC to take the following actions:

- NIST was to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems. As part of its efforts to accomplish this, NIST identified cybersecurity standards for these systems and the need to develop guidelines for organizations such as electric companies on how to securely implement smart grid systems. In January 2011,[6] we reported that NIST had identified 11 standards involving cybersecurity that support smart grid interoperability and had issued a first version of a cybersecurity guideline.[7] In February 2012, NIST issued the 2.0 version of the framework that, according to NIST documents, added 22 standards, specifications, and guidelines to the 75 standards NIST recommended as being applicable to the smart grid in the 1.0 version from January 2010.[8] In September 2014, NIST issued the first revision of the cybersecurity guidelines.[9]
- FERC was to adopt standards resulting from NIST's efforts that it deemed necessary to ensure smart grid functionality and interoperability. However, according to FERC officials, the statute did not provide specific additional authority to allow FERC to require utilities or manufacturers of smart grid technologies to follow these standards. As a result, any standards identified and developed through the NIST-led process are voluntary unless regulators use other authorities to indirectly compel utilities and manufacturers to follow them.

[6]GAO-11-117.

[7]NIST Special Publication 1108, *NIST Framework and Roadmap for Smart Grid Interoperability Standards*, Release 1.0, January 2010 and NIST Interagency Report 7628, *Guidelines for Smart Grid Cyber Security*, August 2010.

[8]NIST Special Publication 1108R2, *NIST Framework and Roadmap for Smart Grid Interoperability Standards*, Release 2.0, February 2012.

[9]NIST Interagency Report 7628 Revision 1, *Guidelines for Smart Grid Cyber Security*, September 2014.

Cyber Threats and Vulnerabilities Facing the Electricity Grid

Like threats affecting other critical infrastructures, threats to the electricity industry and its transmission and distribution systems are evolving and growing and can come from a wide array of sources. Risks to cyber-based assets can originate from unintentional or intentional threats. Unintentional threats can be caused by, among other things, natural disasters, defective computer or network equipment, software coding errors, and careless or poorly trained employees. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled insiders, foreign nations engaged in espionage and information warfare, and terrorists.

These adversaries vary in terms of their capabilities, willingness to act, and motives, which can include seeking monetary gain or pursuing a political, economic, or military advantage. For example, adversaries possessing sophisticated levels of expertise and significant resources to pursue their objectives—sometimes referred to as "advanced persistent threats"—pose increasing risks. They make use of various techniques—or exploits—that may adversely affect federal information, computers, software, networks, and operations, such as a denial of service, which prevents or impairs the authorized use of networks, systems, or applications.

The potential impact of these threats is amplified by the connections between industrial control systems, supervisory control and data acquisition (or SCADA) systems, information systems, the Internet, and other infrastructures, which create opportunities for attackers to disrupt critical services, including electrical power. The increased reliance on IT systems and networks also exposes the electric grid to potential and known cybersecurity vulnerabilities. These include

- an increased number of entry points and paths that can be exploited;
- the introduction of new, unknown vulnerabilities resulting from an increased use of new system and network technologies;
- wider access to systems and networks due to increased connectivity; and
- an increased amount of customer information being collected and transmitted, which creates a tempting target for potential attackers.

We and others have also reported that smart grid and related systems have known cyber vulnerabilities. For example, cybersecurity experts have demonstrated that certain smart meters can be successfully attacked, possibly resulting in disruption to the electricity grid. In addition, we have reported that control systems used in industrial settings such as

electricity generation have vulnerabilities that could result in serious damages and disruption if exploited.[10] Further, in 2007, the Department of Homeland Security, in cooperation with the Department of Energy, ran a test that demonstrated that a vulnerability commonly referred to as "Aurora" had the potential to allow unauthorized users to remotely control, misuse, and cause damage to a small commercial electric generator. Moreover, in 2008, the Central Intelligence Agency reported that malicious activities against IT systems and networks have caused disruption of electric power capabilities in multiple regions overseas, including a case that resulted in a multicity power outage.[11] In January 2014, the Director of National Intelligence, testified that industrial control systems and SCADA systems used in electrical power distribution and other industries provided an enticing target to malicious actors and that, although newer architectures provide flexibility, functionality, and resilience, large segments remain vulnerable to attack, which might cause significant economic or human impact. Further, in 2015 the Director testified that studies asserted that foreign cyber actors were developing means to access industrial control systems remotely, including those that manage critical infrastructures such as electric power grids. As government, private sector, and personal activities continue to move to networked operations, the threat will continue to grow.

Cyber incidents continue to affect the electric industry. For example, the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team noted that the number of reported cyber incidents affecting control systems of companies in the electricity subsector increased from 3 in 2009 to 25 in 2011. The response team reported that the energy sector, which includes the electricity subsector, led all others in fiscal year 2014 with 79 reported incidents. Reported incidents affecting the electricity subsector have had a variety of impacts, including hacks into smart meters to steal power, failure in control systems devices requiring power plants to be shut down, and malicious software disabling safety monitoring systems.

[10]GAO-07-1036.

[11]The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: May 29, 2009).

Actions Have Been Taken to Secure the Electricity Grid, but Continued Attention Is Required

As we have previously reported, multiple entities have taken steps to help secure the electricity grid, including NERC, NIST, FERC, and the Departments of Homeland Security and Energy. For example, NERC developed critical infrastructure standards for protecting electric utility–critical and cyber-critical assets. These standards established requirements for key cybersecurity-related controls: the identification of critical cyber assets, security management, personnel and training, electronic "security perimeters," physical security of critical cyber assets, systems security management, incident reporting and response planning, and recovery plans for critical cyber assets. In December 2011 we reported that NERC's cybersecurity standards, along with supplementary guidance, were substantially similar to NIST guidance applicable at the time to federal agencies.[12]

NERC had also published security guidelines for companies to consider for protecting electric infrastructure systems, although these guidelines were voluntary and typically not checked for compliance. For example, some of this guidance was intended to assist entities in identifying and developing a list of critical cyber assets. As of October 2015, NERC listed about 30 critical infrastructure protection standards for cybersecurity, some of which were subject to enforcement, some which were subject to future enforcement, and some which were pending regulatory filing or approval. NERC also had enforced compliance with mandatory cybersecurity standards through its Compliance Monitoring and Enforcement Program, including assessing monetary penalties for violations.

NIST, in accordance with its responsibilities under the Energy Independence and Security Act of 2007, has identified cybersecurity standards for smart grid systems. Specifically, in August 2010 NIST had identified 11 such standards and issued the first version of a cybersecurity guideline.[13] As we reported in January 2011, NIST's guidelines largely addressed key cybersecurity elements, with the exception of the risk of attacks using both cyber and physical means—an element essential to securing smart grid systems. We recommended that

[12]GAO-12-92.

[13]GAO-11-117.

NIST finalize its plan and schedule for incorporating the missing elements into its guidelines. In 2014, NIST issued updated guidelines, which address the relationship of smart grid cybersecurity to cyber-physical attacks and cybersecurity testing and certification.[14] In addition, it describes the relationship of smart grid cybersecurity to NIST's cybersecurity framework that was issued in February 2014.[15] This framework, which was developed in accordance with Executive Order 13636,[16] is to enable organizations—regardless of size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improving the cybersecurity and resilience of critical infrastructure.

FERC had also taken several actions, including reviewing and approving NERC's critical infrastructure protection standards in 2008. It had also directed NERC to make changes to the standards to improve cybersecurity protections. However, in 2012 the FERC Chairman stated that many of the outstanding directives had not been incorporated into the standards. We also noted in our January 2011 report that FERC had begun reviewing smart grid standards identified by NIST, but declined to adopt them due to insufficient consensus.

The Department of Homeland Security, in its capacity as the lead federal agency for cyber-critical infrastructure protection, had issued recommended practices to reduce risks to industrial control systems in critical infrastructure sectors, including the electricity subsector. The department has also provided on-site support to respond to and analyze security incidents and shared actionable intelligence, vulnerability information, and threat analysis with companies in the electricity subsector. In addition, the department, in accordance with Executive Order 13636, established a program to promote the adoption of the NIST cybersecurity framework.

As the lead agency responsible for critical infrastructure protection efforts in the energy sector, the Department of Energy, as we reported in December 2011, was involved in efforts to assist the electricity subsector in the development, assessment, and sharing of cybersecurity standards,

[14]NIST Interagency Report 7628 Revision 1, *Guidelines for Smart Grid Cybersecurity*, September 2014.

[15]NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0 (Feb. 12, 2014).

[16]Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

according to department officials.[17] In addition, the department has created sector-specific guidance to assist the sector in implementing the NIST cybersecurity framework. The guidance includes sections that explain framework concepts for its application, identify example resources that may support framework use, provide a general approach to framework implementation and identify an example of a tool-specific approach to implementing the framework.

Challenges Existed to Securing Electricity Systems and Networks

In our January 2011 report we identified a number of key challenges that industry and government stakeholders faced in securing the systems and networks supporting the electricity grid.[18]

- *Monitoring implementation of cybersecurity standards.* Best practices for information security call for monitoring the extent to which security controls have been implemented. In our report, we noted that FERC had not developed an approach coordinated with other regulators to monitor, at a high level, the extent to which industry follows the voluntary smart grid standards it adopts. We recommended that FERC, in coordination with state regulators and groups that represent utilities subject to less FERC and state regulation, periodically evaluate the extent to which utilities and manufacturers are following voluntary interoperability and cybersecurity standards and develop strategies for addressing any gaps in compliance with standards that are identified as a result of this evaluation. However, FERC has not implemented this recommendation. While FERC has reported that it has taken steps to collaborate with stakeholders, it has not taken steps to determine the extent to which the voluntary standards have been integrated into products or whether they are effective. Monitoring such efforts would help FERC and other regulators know if their approach to standards setting is effective or if changes are needed.

- *Clarifying regulatory responsibilities.* Experts we spoke with during the course of our review in 2011 expressed concern that there was a lack of clarity about the division of responsibility between federal and state regulators, particularly regarding cybersecurity. While jurisdictional responsibility has historically been determined by whether a

[17]GAO-12-92.

[18]GAO-11-117.

technology is located on the transmission or distribution system, experts raised concerns that smart grid technology may blur these lines because, for example, devices deployed on parts of the grid traditionally subject to state jurisdiction could, in the aggregate, affect the reliability of the transmission system, which falls under federal jurisdiction. Experts also noted concern about the ability of regulatory bodies to respond quickly to evolving cybersecurity threats. Clarifying these responsibilities could help improve the effectiveness of efforts to protect smart grid technology from cyber threats.

- *Taking a comprehensive approach to cybersecurity.* To secure their systems and information, entities should adopt an integrated, organization-wide program for managing information security risk. Such an approach helps ensure that risk management decisions are aligned strategically with the organization's mission and security controls are effectively implemented. However, as we reported in 2011, experts told us that the existing federal and state regulatory environment had created a culture within the utility industry of focusing on compliance with regulatory requirements instead of one focused on achieving comprehensive and effective cybersecurity. By taking such a comprehensive approach, utilities could better mitigate cybersecurity risk.

- *Ensuring that smart grid systems have built-in security features.* Information systems should be securely configured, including having the ability to record events that take place on networks to allow for detecting and analyzing potential attacks. Nonetheless, experts told us that certain currently available smart meters had not been designed with a strong security architecture and lacked important security features, such as event logging.[19] By ensuring that smart grid systems are securely designed, utilities could enhance their ability to detect and analyze attacks, reducing the risk that attacks will succeed and helping to prevent them from recurring.

- *Effectively sharing cybersecurity information.* Information sharing is a key element in the model established by federal policy for protecting critical infrastructure. However, the electric industry lacked an effective mechanism to disclose information about cybersecurity vulnerabilities, incidents, threats, lessons learned, and best practices.

[19]Event logging is the ability of an IT system to record events occurring within an organization's systems and networks, including those related to computer security.

For example, experts we spoke with stated that while the industry had an information sharing center, it did not fully address these information needs. Establishing quality processes for information sharing will help provide utilities with the information needed to adequately protect cyber assets against attackers.

- *Establishing metrics for evaluating cybersecurity.* Metrics are important for comparing the effectiveness of competing cybersecurity solutions and determining what mix of solutions will make the most secure system. The electric industry, however, was challenged by a lack of cybersecurity metrics, making it difficult to determine the extent to which investments in cybersecurity improve the security of smart grid systems. Developing such metrics could provide utilities with key information for making informed and cost-effective decisions on cybersecurity investments.

In our January 2011 report, we recommended that FERC, working with NERC as appropriate, assess whether any cybersecurity challenges identified in our report should be addressed in commission cybersecurity efforts.

Since that time, FERC took the following actions. First, in 2011, it began evaluating whether cybersecurity challenges, including those identified in our report, should be addressed under the agency's existing cyber security authority and efforts. As a part of this effort, the commission directed NERC to revise the electricity industry's critical infrastructure protection (CIP) standards with the aim of addressing, among other things, cybersecurity challenges identified in our report. In November 2013, NERC issued updated CIP standards to address these and other cybersecurity challenges. Second, the commission held a technical conference in 2011 in which it solicited feedback from industry stakeholders to help inform the agency's cybersecurity efforts. Third, in September 2012, the commission established an Office of Energy Infrastructure Security, which is to, among other things, help mitigate cyber security threats to electricity industry facilities, and to improve cybersecurity information sharing.

In summary, as they become increasingly reliant on computerized technologies, the electricity industry’s systems and networks are susceptible to an evolving array of cyber-based threats. Key entities, including NERC and FERC, are critical to approving and disseminating cybersecurity guidance and standards, while NIST, DHS, and the Department of Energy have additional roles to play in providing guidance

and providing other forms of support for protecting the sector against cyber threats. Moreover, without monitoring the implementation of voluntary cybersecurity standards in the industry, FERC does not know the extent to which such standards have been adopted or whether they are effective. Given the increasing use of information and communications technology in the electricity subsector and the evolving nature of cyber threats, continued attention can help mitigate the risk these threats pose to the electricity grid.

Chairman Weber, Chairwoman Comstock, Ranking Members Grayson and Lipinski, and Members of the Subcommittees, this concludes my prepared statement. I would be happy to answer any questions you may have at this time.

Contact and Acknowledgments

If you or your staffs have any questions about this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other staff who contributed to this statement include Franklin J. Rusco, Director; Michael W. Gilmore; Bradley W. Becker; Kenneth A. Johnson; Jon R. Ludwigson; Lee McCracken; Jonathan Wall; and Jeffrey W. Woodward.

Biography

Gregory Wilshusen is Director of Information Security Issues at GAO, where he leads cybersecurity and privacy-related studies and audits of the federal government and critical infrastructure. He has over 30 years of auditing, financial management, and information systems experience. Prior to joining GAO in 1997, Mr. Wilshusen held a variety of public and private sector positions. He was a senior systems analyst at the Department of Education. He also served as the Controller for the North Carolina Department of Environment, Health, and Natural Resources, and held senior auditing positions at Irving Burton Associates, Inc. and the U.S. Army Audit Agency. He's a certified public accountant, certified internal auditor, and certified information systems auditor. He holds a B.S. degree in business administration (accounting) from the University of Missouri and an M.S. in information management from George Washington University's School of Engineering and Applied Sciences.