United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at 10:15 a.m. EST
Tuesday, February 28, 2012

CYBERSECURITY

Challenges in Securing the Modernized Electricity Grid

Statement of Gregory C. Wilshusen, Director
Information Security Issues

David C. Trimble, Director
Natural Resources and Environment

February 2012

CYBERSECURITY

Challenges in Securing the Modernized Electricity Grid

GAO Highlights

Accountability * Integrity * Reliability

Highlights of GAO-12-507T, a testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

Why GAO Did This Study

The electric power industry is increasingly incorporating information technology (IT) systems and networks into its existing infrastructure as part of nationwide efforts—commonly referred to as the "smart grid"—aimed at improving reliability and efficiency and facilitating the use of alternative energy sources such as wind and solar. Smart grid technologies include metering infrastructure ("smart meters") that enable two-way communication between customers and electricity utilities, smart components that provide system operators with detailed data on the conditions of transmission and distribution systems, and advanced methods for controlling equipment. The use of these systems can bring a number of benefits, such as fewer and shorter outages, lower electricity rates, and an improved ability to respond to attacks on the electric grid. However, this increased reliance on IT systems and networks also exposes the grid to cybersecurity vulnerabilities, which can be exploited by attackers. Moreover, for nearly a decade, GAO has identified the protection of systems supporting our nation's critical infrastructure—which include the electric grid—as a governmentwide high-risk area.

GAO is providing a statement describing (1) cyber threats facing cyber-reliant critical infrastructures and (2) key challenges to securing smart grid systems and networks. In preparing this statement, GAO relied on its previously published work in this area.

View GAO-12-507T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or David C. Trimble at (202) 512-3841 or trimbled@gao.gov.

What GAO Found

The threats to systems supporting critical infrastructures are evolving and growing. In a February 2011 testimony, the Director of National Intelligence noted that there had been a dramatic increase in cyber activity targeting U.S. computers and systems in the previous year, including a more than tripling of the volume of malicious software since 2009. Varying types of threats from numerous sources can adversely affect computers, software, networks, organizations, entire industries, and the Internet itself. These include both unintentional and intentional threats, and may come in the form of targeted or untargeted attacks from criminal groups, hackers, disgruntled employees, hostile nations, or terrorists. The interconnectivity between information systems, the Internet, and other infrastructures can amplify the impact of these threats, potentially affecting the operations of critical infrastructures, the security of sensitive information, and the flow of commerce. Moreover, the smart grid's reliance on IT systems and networks exposes the electric grid to potential and known cybersecurity vulnerabilities, which could be exploited by attackers.

As GAO reported in January 2011, securing smart grid systems and networks presented a number of key challenges that required attention by government and industry. These included:

- **A lack of a coordinated approach to monitor industry compliance with voluntary standards.** The Federal Energy Regulatory Commission (FERC) is responsible for regulating aspects of the electric power industry, which includes adopting cybersecurity and other standards it deems necessary to ensure smart grid functionality and interoperability. However, FERC had not, in coordination with other regulators, developed an approach to monitor the extent to which industry will follow the voluntary smart grid standards it adopts. As a result, it would be difficult for FERC and other regulators to know whether a voluntary approach to standards setting is effective.
- **A lack of security features built into smart grid devices.** According to a panel of experts convened by GAO, smart meters had not been designed with a strong security architecture and lacked important security features. Without securely designed systems, utilities would be at risk of attacks occurring undetected.
- **A lack of an effective information-sharing mechanism within the electricity industry.** While the industry has an information-sharing center, it had not fully addressed the need for sharing cybersecurity information in a safe and secure way. Without quality processes for sharing information, utilities may lack information needed to protect their assets against attackers.
- **A lack of metrics for evaluating cybersecurity.** The industry lacked metrics for measuring the effectiveness of cybersecurity controls, making it difficult to measure the extent to which investments in cybersecurity improve the security of smart grid systems. Until such metrics are developed, utilities may not invest in security in a cost-effective manner or be able to make informed decisions about cybersecurity investments.

GAO made several recommendations to FERC aimed at addressing these challenges. The commission agreed with these recommendations and described steps it is taking to implement them.

Chairman Stearns, Ranking Member DeGette, and Members of the Subcommittee:

Thank you for the opportunity to testify at today's hearing on assessments of security for the smart grid.

As you know, the electric power industry is increasingly incorporating information technology (IT) systems and networks into its existing infrastructure (e.g., electricity networks including power lines and customer meters) as part of nationwide efforts—commonly referred to as the "smart grid"—aimed at improving reliability and efficiency and facilitating the use of alternative energy sources (e.g., wind and solar). Along with these anticipated benefits, however, cybersecurity and industry experts have expressed concern that, if not implemented securely, smart grid systems will be vulnerable to attacks that could result in widespread loss of electrical services essential to maintaining our national economy and security.

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

In our testimony today, we will describe (1) cyber threats facing cyber-reliant critical infrastructures, which include the electric grid,[2] and (2) key challenges to securing smart grid systems and networks. In preparing this statement in February 2012, we relied on our previous work in this area, including a review of efforts to secure the smart grid and associated challenges.[3] The products upon which this statement is based contain

[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 high-risk area since 1997; in 2003, we expanded this high-risk area to include protecting systems supporting our nation's critical infrastructure—referred to as cyber-critical infrastructure protection, or cyber CIP. See, most recently, GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

[2]Federal policy established 18 critical infrastructure sectors: banking and finance; chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; food and agriculture; government facilities; health care and public health; information technology; national monuments and icons; nuclear reactors, materials, and waste; postal and shipping; transportation systems; and water.

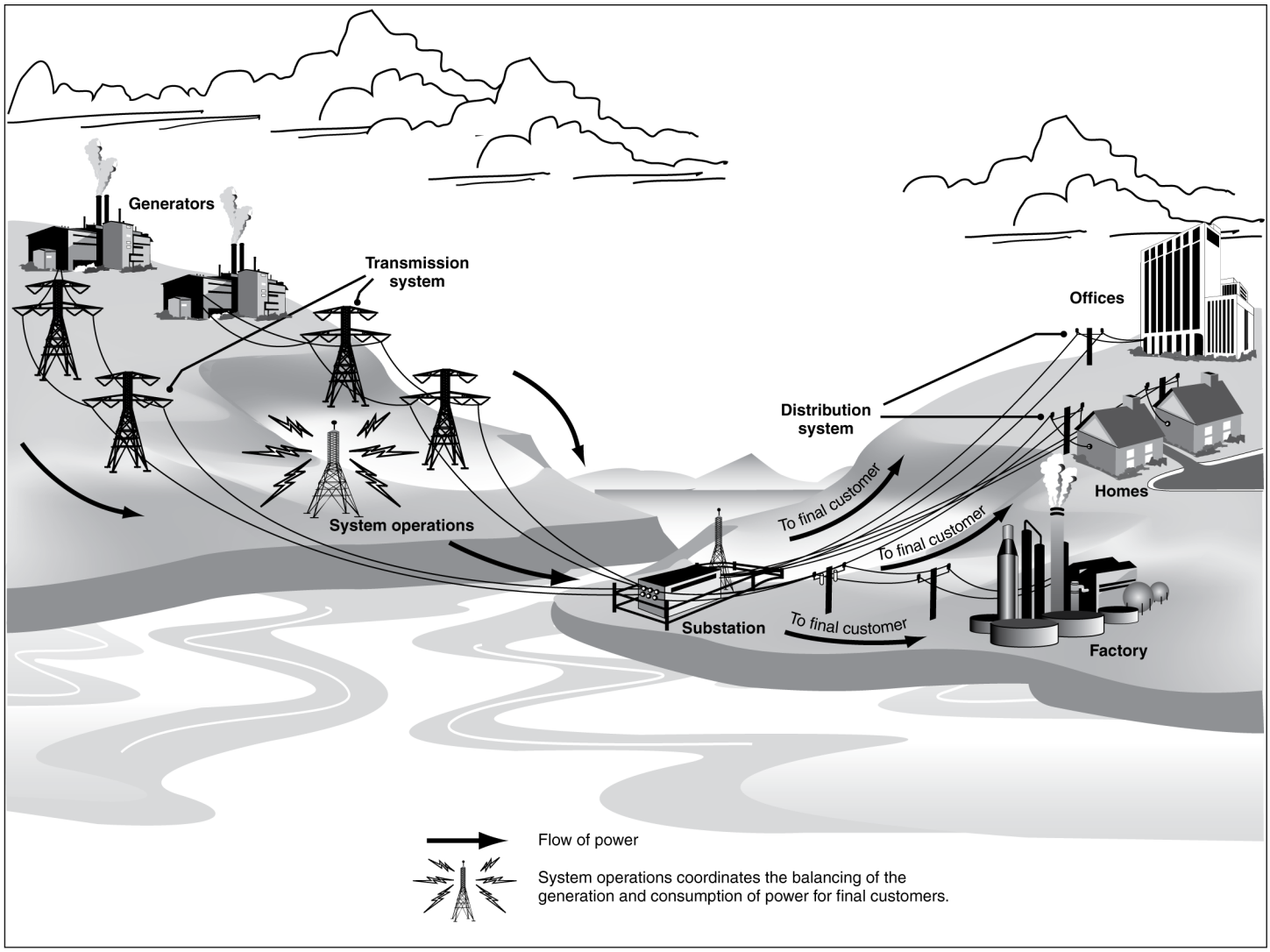
[3]GAO, *Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed*, GAO-11-117 (Washington, D.C.: Jan. 12, 2011).

detailed overviews on the scope of our reviews and the methodology we used. The work on which this statement is based was performed 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. We believe that the evidence obtained provided 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 analysis.

Utilities 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.[4] As we have previously reported, the effective functioning of the electricity industry is highly dependent on these control systems.[5] However, for many years, aspects of the electricity network lacked (1) adequate 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.

Smart Grid Aims to Modernize 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.

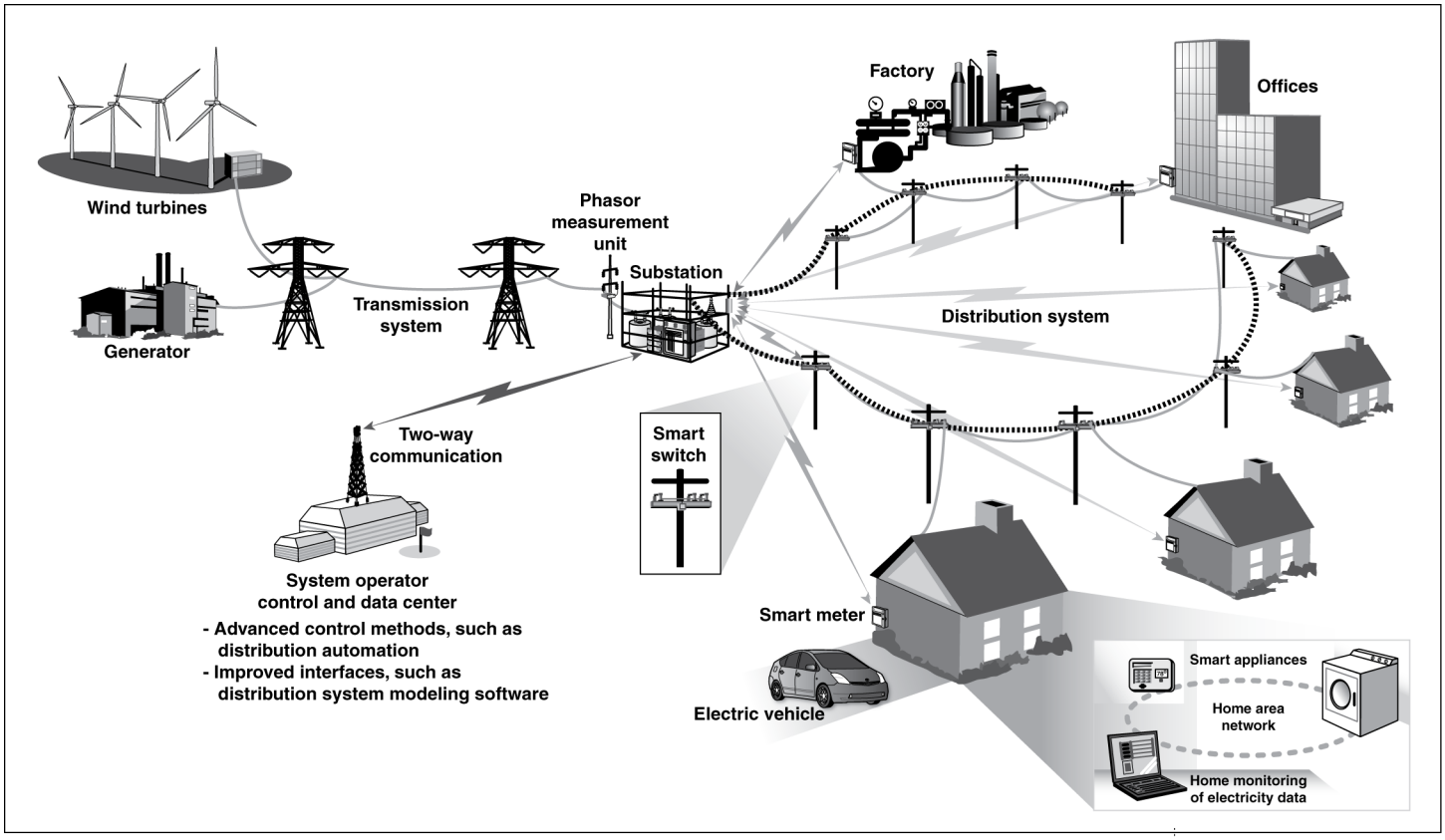
This vision—the smart grid—would increase the use of IT systems and networks and two-way communication to automate actions that system operators formerly had to make manually. Smart grid modernization is an ongoing process, and initiatives have commonly involved installing advanced metering infrastructure (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 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 that communicate with each other to reroute electricity around a

[4]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.

[5]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).

troubled line and high-resolution, time-synchronized monitors—called phasor measurement units—on the transmission system. Figure 2 illustrates one possible smart grid configuration, though utilities making smart grid investments may opt for alternative configurations depending on cost, customer needs, and local conditions.

Figure 2: Common Smart Grid Components



Source: GAO analysis.

According to the National Energy Technology Laboratory, a Department of Energy (DOE) national laboratory supporting smart grid efforts, smart grid systems fall into several different categories:

- Integrated communications, such as broadband over power line communication technologies or wireless communications technologies.
- Advanced components, such as smart switches, transformers, cables, and other devices; storage devices, such as plug-in hybrid electric

vehicles and advanced batteries; and grid-friendly smart home appliances.
- Advanced control methods, including real-time monitoring and control of substation and distribution equipment.
- Sensing and measurement technologies, such as smart meters and phasor measurement units.
- Improved interfaces and decision support, which includes software tools to analyze the health of the electricity system and real-time digital simulators to study and test systems.

The use of smart grid systems may have a number of benefits, including improved reliability from fewer and shorter outages, downward pressure on electricity rates resulting from the ability to shift peak demand, an improved ability to shift to 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 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 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.

Federal Smart Grid Activities

The Energy Independence and Security Act of 2007 (EISA)[6] established federal support for the modernization of the electricity grid and required actions by a number of federal agencies, including the National Institute of Standards and Technology (NIST), FERC, and DOE. With regard to cybersecurity, the act called for 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 planned to identify cybersecurity standards for these systems and also identified the need to develop guidelines for organizations such as electric companies on how to securely implement smart grid systems. In January 2011,[7] 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.[8]
- FERC was to adopt standards resulting from NIST's efforts that it deemed necessary to ensure smart grid functionality and interoperability.

The act also authorized DOE to establish two initiatives to facilitate the development of industry smart grid efforts. These were the Smart Grid Investment Grant Program and the Smart Grid Regional Demonstration Initiative. DOE made $3.5 billion and $685 million of American Recovery and Reinvestment Act ("Recovery Act")[9] funds available for these two initiatives, respectively. The Smart Grid Investment Grant Program provided grant awards to utilities in multiple states to stimulate the rapid deployment and integration of smart grid technologies, while the Smart Grid Regional Demonstration Initiative was to fund regional demonstrations to verify technology viability, quantify costs and benefits, and validate new business models for the smart grid at a scale that can be readily adopted around the country. The federal government has also

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

[7]GAO-11-117.

[8]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.

[9]Pub. L. No. 111-5 (Feb. 17, 2009).

undertaken various other smart-grid-related initiatives, including funding technical research and development, data collection, and coordination activities.

In January 2012, the DOE Inspector General reported that cybersecurity plans submitted by Smart Grid Investment Grant Program recipients were not always complete or they did not describe intended security controls in sufficient detail.[10] The report also stated that DOE officials approved cybersecurity plans for smart grid projects even though some of the plans contained shortcomings that could result in poorly implemented controls. The report recommended, among other things, that DOE ensure that grantees' cybersecurity plans were complete, including thorough descriptions of potential security risks and related mitigation through necessary controls. The responsible DOE office stated that it will continue to ensure that the security plans are complete and are implemented properly.

Smart Grid Is Potentially Vulnerable to a Variety of Cyber Threats

Threats to systems supporting critical infrastructure—which includes the electricity industry and its transmission and distribution systems—are evolving and growing. In February 2011, the Director of National Intelligence testified that, in the past year, there had been a dramatic increase in malicious cyber activity targeting U.S. computers and networks, including a more than tripling of the volume of malicious software since 2009.[11] Different types of cyber threats from numerous sources may adversely affect computers, software, networks, organizations, entire industries, or the Internet. Cyber threats can be unintentional or intentional. Unintentional threats can be caused by software upgrades or maintenance procedures that inadvertently disrupt systems. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, and terrorists. Moreover, these groups have a wide array of

[10]U.S. Department of Energy, Office of Inspector General, Office of Audits and Inspections, *Audit Report: The Department's Management of the Smart Grid Investment Grant Program*, OAS-RA-12-04 (Washington, D.C.: Jan. 20, 2012).

[11]Director of National Intelligence, *Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community*, statement before the Senate Select Committee on Intelligence (Feb. 16, 2011).

cyber exploits at their disposal. Table 1 provides descriptions of common types of cyber exploits.

Table 1: Common Cyber Exploits

Type of exploit	Description
Cross-site scripting	An attack that uses third-party web resources to run script within the victim's web browser or scriptable application. This occurs when a browser visits a malicious website or clicks a malicious link. The most dangerous consequences occur when this method is used to exploit additional vulnerabilities that may permit an attacker to steal cookies (data exchanged between a web server and a browser), log key strokes, capture screen shots, discover and collect network information, and remotely access and control the victim's machine.
Denial-of-service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Distributed denial-of-service	A variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Logic bomb	A piece of programming code intentionally inserted into a software system that will cause a malicious function to occur when one or more specified conditions are met.
Phishing	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users to direct them to a fake website that requests information.
Passive wiretapping	The monitoring or recording of data, such as passwords transmitted in clear text, while they are being transmitted over a communications link. This is done without altering or affecting the data.
SQL injection	An attack that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database.
Trojan horse	A computer program that appears to have a useful function but also has a hidden and potentially malicious function that evades security mechanisms by, for example, masquerading as a useful program that a user would likely execute.
Virus	A computer program that can copy itself and infect a computer without the permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.
War driving	The method of driving through cities and neighborhoods with a wireless-equipped computer—sometimes with a powerful antenna—searching for unsecured wireless networks.
Worm	A self-replicating, self-propagating, self-contained program that uses network mechanisms to spread itself. Unlike computer viruses, worms do not require human involvement to propagate.
Zero-day exploit	An exploit that takes advantage of a security vulnerability previously unknown to the general public. In many cases, the exploit code is written by the same person who discovered the vulnerability. By writing an exploit for the previously unknown vulnerability, the attacker creates a potent threat since the compressed time frame between public discoveries of both makes it difficult to defend against.

Source: GAO analysis of data from NIST, the United States Computer Emergency Readiness Team, and industry reports.

The potential impact of these threats is amplified by the connectivity between information systems, the Internet, and other infrastructures, creating opportunities for attackers to disrupt critical services, including electrical power. For example, in May 2008, we reported that the corporate network of the Tennessee Valley Authority (TVA)—the nation's largest public power company, which generates and distributes power in an area of about 80,000 square miles in the southeastern United States—

contained security weaknesses that could lead to the disruption of control systems networks and devices connected to that network.[12] We made 19 recommendations to improve the implementation of information security program activities for the control systems governing TVA's critical infrastructures and 73 recommendations to address specific weaknesses in security controls. TVA concurred with the recommendations and has taken steps to implement them. As government, private sector, and personal activities continue to move to networked operations, the threat will continue to grow.

We have reported[13] that cyber incidents can affect the operations of energy facilities, as the following examples illustrate:

- **Stuxnet.** In July 2010, a sophisticated computer attack known as Stuxnet was discovered. It targeted control systems used to operate industrial processes in the energy, nuclear, and other critical sectors. It is designed to exploit a combination of vulnerabilities to gain access to its target and modify code to change the process.
- **Browns Ferry power plant.** In August 2006, two circulation pumps at Unit 3 of the Browns Ferry, Alabama, nuclear power plant failed, forcing the unit to be shut down manually. The failure of the pumps was traced to excessive traffic on the control system network, possibly caused by the failure of another control system device.
- **Northeast power blackout.** In August 2003, failure of the alarm processor in the control system of FirstEnergy, an Ohio-based electric utility, prevented control room operators from having adequate situational awareness of critical operational changes to the electrical grid. When several key transmission lines in northern Ohio tripped due to contact with trees, they initiated a cascading failure of 508 generating units at 265 power plants across eight states and a Canadian province.
- **Davis-Besse power plant**. The Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as Slammer infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly 5 hours. In addition, the plant's process computer failed, and it took about 6 hours for it to become available again.

[12]GAO, *Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks*, GAO-08-526 (Washington, D.C.: May 21, 2008).

[13]GAO-07-1036 and GAO-12-92.

Smart Grid Faces Cybersecurity Vulnerabilities

While presenting significant potential benefits, the smart grid vision and its increased reliance on IT systems and networks also expose the electric grid to potential and known cybersecurity vulnerabilities, which could be exploited by a wide array of cyber threats. This creates an increased risk to the smooth and reliable operation of the grid. As we and others have reported,[14] these vulnerabilities include

- an increased number of entry points and paths that can be exploited by potential adversaries and other unauthorized users;
- the introduction of new, unknown vulnerabilities due to 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, providing incentives for adversaries to attack these systems and potentially putting private information at risk of unauthorized disclosure and use.

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.[15] Further, in 2009, the Department of Homeland Security, in cooperation with DOE, 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.[16]

[14]GAO-11-117.

[15]GAO-07-1036.

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

Securing Smart Grid Systems and Networks Presents Challenges

In our January 2011 report, we identified a number of key challenges that industry and government stakeholders faced in ensuring the cybersecurity of the systems and networks that support our nation's electricity grid.[17] Among others, these challenges included the following:

- *Lack of a coordinated approach to monitor whether industry follows voluntary standards.* As mentioned above, under EISA, FERC is responsible for adopting cybersecurity and other standards that it deems necessary to ensure smart grid functionality and interoperability. However, FERC had not developed an approach coordinated with other regulators to monitor, at a high level, the extent to which industry will follow the voluntary smart grid standards it adopts. There had been initial efforts by regulators to share views, through, for example, a collaborative dialogue between FERC and the National Association of Regulatory Utility Commissioners (NARUC), which had discussed the standards-setting process in general terms. Nevertheless, according to officials from FERC and NARUC, FERC and the state public utility commissions had not established a joint approach for monitoring how widely voluntary smart grid standards are followed in the electricity industry or developed strategies for addressing any gaps. Moreover, FERC had not coordinated in such a way with groups representing public power or cooperative utilities, which are not routinely subject to FERC's or the states' regulatory jurisdiction for rate setting. We noted that without a good understanding of whether utilities and manufacturers are following smart grid standards, it would be difficult for FERC and other regulators to know whether a voluntary approach to standards setting is effective or if changes are needed.[18]

[17]GAO-11-117.

[18]In an order issued on July 19, 2011, FERC reported that it had found insufficient consensus to institute a rulemaking proceeding to adopt Smart Grid interoperability standards identified by NIST as ready for consideration by regulatory authorities. While FERC dismissed the rulemaking, it encouraged utilities, smart grid product manufacturers, regulators, and other smart grid stakeholders to actively participate in the NIST interoperability framework process to work on the development of interoperability standards and to refer to that process for guidance on smart grid standards. Despite this result, we believe our recommendations to FERC in GAO-11-117, with which FERC concurred, remain valid and should be acted upon as consensus is reached and standards adopted.

- *Lack of security features being built into certain smart grid systems.* Security features had not been consistently built into smart grid devices. For example, according to experts from a panel convened by GAO, currently available smart meters had not been designed with a strong security architecture and lacked important security features, such as event logging[19] and forensics capabilities, which are needed to detect and analyze attacks. In addition, these experts stated that smart grid home area networks—used for managing the electricity usage of appliances and other devices in the home—did not have adequate security built in, thus increasing their vulnerability to attack. Without securely designed smart grid systems, utilities may not be able to detect and analyze attacks, increasing the risk that attacks would succeed and utilities would be unable to prevent them from recurring.
- *Lack of an effective mechanism for sharing cybersecurity information within the electricity industry.* The electricity industry lacked an effective mechanism to disclose information about smart grid cybersecurity vulnerabilities, incidents, threats, lessons learned, and best practices in the industry. For example, experts stated that while the industry has an information-sharing center, it had not fully addressed these information needs. According to these experts, information regarding incidents such as both successful and unsuccessful attacks must be able to be shared in a safe and secure way; this is crucial to avoid publicly revealing the reported organization and penalizing entities actively engaged in corrective action. Such information sharing across the industry could provide important information regarding the level of attempted attacks and their methods, which could help grid operators better defend against them. In developing an approach to cybersecurity information sharing, the industry could draw upon the practices and approaches of other industries. Without quality processes for information sharing, utilities may not have the information needed to adequately protect their assets against attackers.
- *Lack of industry metrics for evaluating cybersecurity.* The electricity industry was also challenged by a lack of cybersecurity metrics, making it difficult to measure the extent to which investments in cybersecurity improve the security of smart grid systems. Experts noted that while such metrics[20] are difficult to develop, they could help

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

[20]Metrics can be used for, among other things, measuring the effectiveness of cybersecurity controls for detecting and blocking cyber attacks.

in comparing the effectiveness of competing solutions and determining what mix of solutions best secure systems. Further, our panel of experts noted that having metrics would help utilities develop a business case for cybersecurity by helping to show the return on a particular investment. Until such metrics are developed, increased risk exists that utilities will not invest in security in a cost-effective manner or be able to have the information needed to make informed decisions about their cybersecurity investments.

Accordingly, in our January 2011 report, we made multiple recommendations to FERC, including that it develop an approach to coordinating with state regulators to evaluate the extent to which utilities and manufacturers are following voluntary smart grid standards and develop strategies for addressing any gaps in compliance with standards that are identified as a result. We further recommended that FERC, working with NERC as appropriate, assess whether commission efforts should address any of the cybersecurity challenges identified in our report. FERC agreed with our recommendations and described steps the commission intended to take to address them. We are currently working with FERC officials to determine the status of their efforts to address these recommendations.

Concluding Observations

In summary, the electricity industry is in the midst of a major transformation as a result of smart grid initiatives and this has led to significant investments by many entities, including utilities, private companies, and the federal government. While these initiatives hold the promise of significant benefits, including a more resilient electric grid, lower energy costs, and the ability to tap into alternative sources of power, the prevalence of cyber threats aimed at the nation's critical infrastructure and the cyber vulnerabilities arising from the use of new technologies highlight the importance of securing smart grid systems. In particular, it will be important for federal regulators and other stakeholders to work closely with the private sector to address key cybersecurity challenges posed by the transition to smart grid technology. While no system can be made 100 percent secure, proven security strategies could help reduce risk to an acceptable level.

Chairman Stearns, Ranking Member DeGette, and Members of the Subcommittee, this completes our statement. We would be happy to answer any questions you have at this time.

Contact and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or David C. Trimble at (202) 512-3841 or trimbled@gao.gov. Other key contributors to this statement include Michael Gilmore (Assistant Director), Jon R. Ludwigson (Assistant Director), Paige Gilbreath, Barbarol J. James, and Lee A. McCracken.