

January 2011

# ELECTRICITY GRID MODERNIZATION

Progress Being Made  
on Cybersecurity  
Guidelines, but Key  
Challenges Remain to  
be Addressed



G A O

Accountability \* Integrity \* Reliability

## Why GAO Did This Study

The electric industry is increasingly incorporating information technology (IT) systems into its operations as part of nationwide efforts—commonly referred to as smart grid—to improve reliability and efficiency. There is concern that if these efforts are not implemented securely, the electric grid could become more vulnerable to attacks and loss of services. To address this concern, the Energy Independence and Security Act of 2007 (EISA) provided the National Institute of Standards and Technology (NIST) and Federal Energy Regulatory Commission (FERC) with responsibilities related to coordinating the development and adoption of smart grid guidelines and standards.

GAO was asked to (1) assess the extent to which NIST has developed smart grid cybersecurity guidelines; (2) evaluate FERC’s approach for adopting and monitoring smart grid cybersecurity and other standards; and (3) identify challenges associated with smart grid cybersecurity. To do so, GAO analyzed agency documentation, interviewed responsible officials, and hosted an expert panel.

## What GAO Recommends

GAO recommends that NIST finalize its plan and schedule for updating its cybersecurity guidelines to incorporate missing elements, and that FERC develop a coordinated approach to monitor voluntary standards and address any gaps in compliance. Both agencies agreed with these recommendations.

View [GAO-11-117](#) or key components. For more information, contact David A. Powner at (202) 512-9286, [pownerd@gao.gov](mailto:pownerd@gao.gov) or David C. Trimble at (202) 512-3841, [trimbled@gao.gov](mailto:trimbled@gao.gov).

# ELECTRICITY GRID MODERNIZATION

## Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed

### What GAO Found

NIST has developed, and issued in August 2010, a first version of its smart grid cybersecurity guidelines. The agency developed the guidelines—for entities such as electric companies involved in implementing smart grid systems—to provide guidance on how to securely implement such systems. In doing this, NIST largely addressed key cybersecurity elements that it had planned to include in the guidelines, such as an assessment of the cybersecurity risks associated with smart grid systems and the identification of security requirements (i.e., controls) essential to securing such systems. This notwithstanding, NIST did not address an important element essential to securing smart grid systems that it had planned to include—addressing the risk of attacks that use both cyber and physical means. NIST also identified other key elements that surfaced during its development of the guidelines that need to be addressed in future guideline updates. NIST officials said that they intend to update the guidelines to address the missing elements, and have drafted a plan to do so. While a positive step, the plan and schedule are still in draft form. Until the missing elements are addressed, there is an increased risk that smart grid implementations will not be secure as otherwise possible.

In 2010, FERC began a process to consider an initial set of smart grid interoperability and cybersecurity standards for adoption, but has not developed a coordinated approach to monitor the extent to which industry is following these standards. While EISA gives FERC authority to adopt smart grid standards, it does not provide FERC with specific enforcement authority. This means that standards will remain voluntary unless regulators are able to use other authorities—such as the ability to oversee the rates electricity providers charge customers—to enforce them. Additionally, although regulatory fragmentation—the divided regulation over aspects of the industry between federal, state, and local entities—complicates oversight of smart grid interoperability and cybersecurity, FERC has not developed an approach coordinated with other regulators to monitor whether industry is following the voluntary smart grid standards it adopts. FERC officials said they have not yet determined whether or how to do so. Nonetheless, adherence to standards is an important step toward achieving an interoperable and secure electricity system and establishing an approach for coordinating on standards adoption could help address gaps, if they arise.

With respect to challenges to securing smart grid systems, GAO identified the following six key challenges:

<ul style="list-style-type: none"> <li>Aspects of the regulatory environment may make it difficult to ensure smart grid systems’ cybersecurity.</li> </ul>	<ul style="list-style-type: none"> <li>Consumers are not adequately informed about the benefits, costs, and risks associated with smart grid systems.</li> </ul>
<ul style="list-style-type: none"> <li>Utilities are focusing on regulatory compliance instead of comprehensive security.</li> </ul>	<ul style="list-style-type: none"> <li>There is a lack of security features being built into certain smart grid systems.</li> </ul>
<ul style="list-style-type: none"> <li>The electric industry does not have an effective mechanism for sharing information on cybersecurity.</li> </ul>	<ul style="list-style-type: none"> <li>The electricity industry does not have metrics for evaluating cybersecurity.</li> </ul>

---

# Contents

---

<b>Letter</b>		<b>1</b>
	Background	2
	NIST Has Developed and Issued Smart Grid Cybersecurity Guidelines, but They Do Not Address Some Key Cybersecurity Elements	14
	FERC Has Begun Reviewing Initial Smart Grid Standards but Has Not Developed a Coordinated Plan to Monitor Industry's Implementation	17
	Electricity Industry Faces Key Challenges to Securing Smart Grid Systems and Networks	22
	Conclusions	25
	Recommendations for Executive Action	26
	Agency Comments and Our Evaluation	27
<b>Appendix I</b>	<b>Objectives, Scope, and Methodology</b>	<b>30</b>
<b>Appendix II</b>	<b>Other Federal Efforts to Facilitate Smart Grid Implementation</b>	<b>32</b>
<b>Appendix III</b>	<b>Expert Panel Discussion Attendees</b>	<b>35</b>
<b>Appendix IV</b>	<b>Comments from the Department of Commerce</b>	<b>37</b>
<b>Appendix V</b>	<b>Comments from the Federal Energy Regulatory Commission</b>	<b>39</b>
<b>Appendix VI</b>	<b>GAO Contacts and Staff Acknowledgments</b>	<b>42</b>
<b>Related GAO Products</b>		<b>43</b>

---

---

## Tables

Table 1: Categories of Smart Grid Systems as Defined by the National Energy Technology Laboratory	7
Table 2: Key NIST Smart Grid Working Groups	12
Table 3: Other Federal Efforts to Support Smart Grid Implementation	32

---

## Figures

Figure 1: Functions of the Electricity Industry	3
Figure 2: Common Smart Grid Components	6

---

## Abbreviations

DOE	Department of Energy
EISA	Energy Independence and Security Act of 2007
FERC	Federal Energy Regulatory Commission
IT	information technology
NARUC	National Association of Regulatory Utility Commissioners
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
PUC	Public Utility Commission

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



**G A O**

Accountability \* Integrity \* Reliability

**United States Government Accountability Office**  
Washington, DC 20548

---

January 12, 2011

The Honorable Bennie G. Thompson  
Ranking Member  
Committee on Homeland Security  
House of Representatives

The Honorable Yvette D. Clarke  
House of Representatives

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 smart grid—aimed at improving reliability and efficiency and facilitating the use of alternative energy sources (e.g., wind, solar). Despite these anticipated benefits, cybersecurity and industry experts have expressed concern that if smart grid systems are not implemented securely, they will be vulnerable to attacks that could result in widespread loss of electrical services essential to maintaining our national economy and security. Experts have also expressed concern about how well smart grid systems will work together (i.e., interoperate), whether modifications will be needed to achieve interoperability, and the extent to which the cost of modifications will be passed to consumers.

The Energy Independence and Security Act of 2007 (EISA)<sup>1</sup> directed the National Institute of Standards and Technology (NIST) to coordinate development of a framework of, among other things, IT standards for ensuring that smart grid systems and networks are interoperable. As part of its efforts to accomplish this, NIST planned to identify interoperability and cybersecurity standards to ensure such systems and networks interoperate properly and are cybersecure. In addition to these undertakings, NIST also identified the need to develop cybersecurity guidelines, for organizations such as electric companies, on how to securely implement smart grid systems. EISA also directed the Federal Energy Regulatory Commission (FERC)—the primary federal regulator of the electricity system—to adopt those standards (identified as part of the

---

<sup>1</sup>Pub. L. No 110-140, (Dec. 19, 2007).

---

NIST efforts) that it deemed necessary to ensure smart grid functionality and interoperability.

As agreed, our objectives were to (1) assess the extent to which NIST has developed smart grid cybersecurity guidelines; (2) evaluate FERC's efforts to adopt smart grid cybersecurity and other standards and monitor their use by industry; and (3) identify challenges associated with ensuring the cybersecurity of the smart grid.

To accomplish the first objective, we analyzed NIST's plans to develop smart grid cybersecurity guidelines; assessed the agency's efforts to date to carry out the plans; and then compared this information to identify any variances, causes, and potential negative impacts; we also interviewed NIST officials responsible for developing the guidelines and industry stakeholders who are to use them. To accomplish the second objective, we collected and analyzed documentation of FERC plans; interviewed FERC officials; and interviewed representatives from seven state electricity regulatory organizations with smart grid activities of interest and varied locations, sizes, and regulatory structures. For the third objective, we convened, with the assistance of the National Academy of Sciences, a panel of 23 experts in smart grid cybersecurity, including experts from utilities, vendors, manufacturers, researchers, and trade associations.

We conducted this performance audit from November 2009 to January 2011, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit 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. Appendix I contains additional details on our objectives, scope, and methodology.

---

## Background

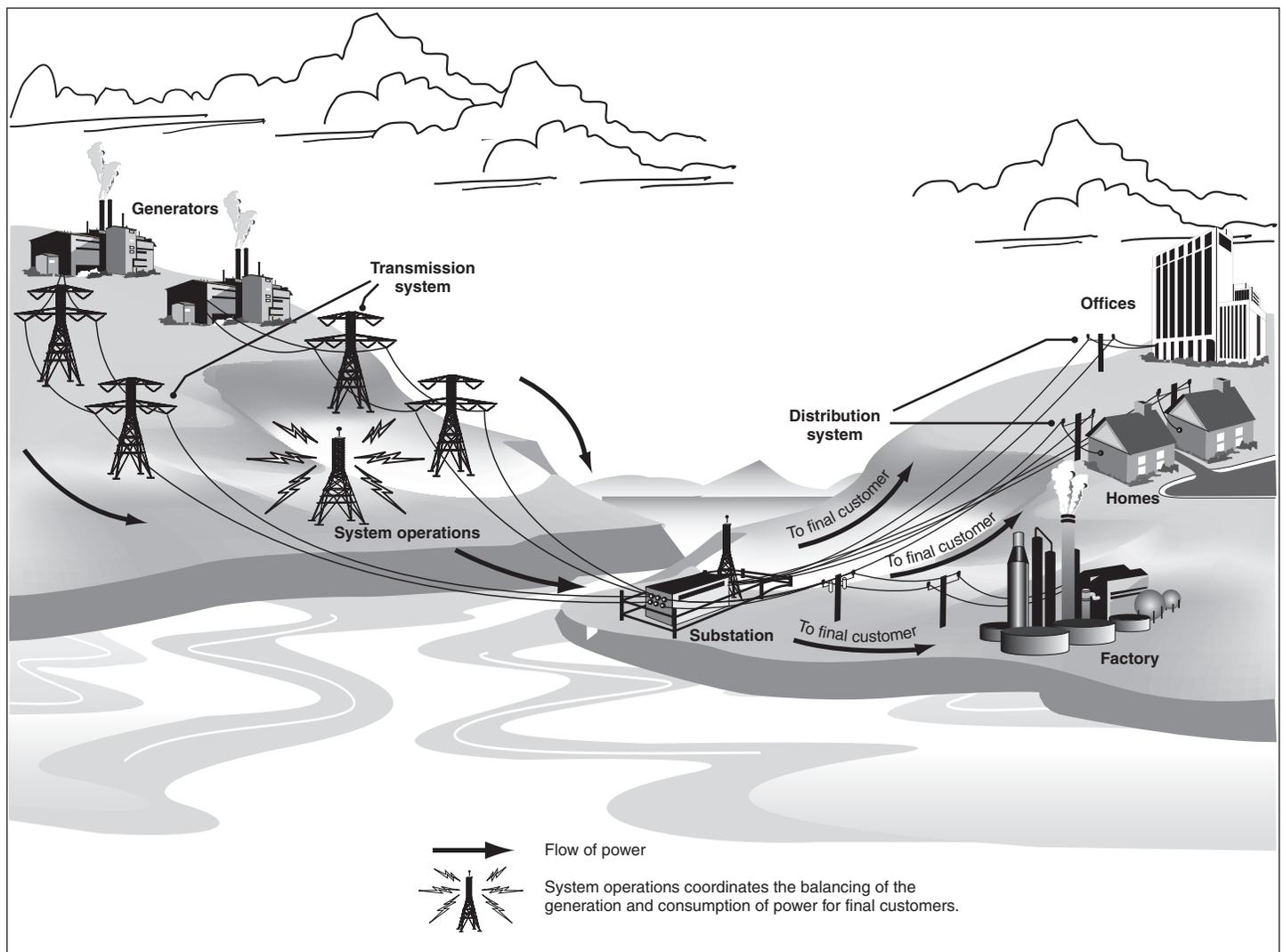
---

### The Electricity Industry

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, commercial 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.<sup>2</sup> As we have previously reported, the effective functioning of the electricity industry is highly dependent on these control systems.<sup>3</sup> See the list of related past GAO products at the end of this report. However, for many years aspects of the electricity network lacked adequate technologies—such as sensors—to allow system operators to understand key information to detect how much electricity was flowing on distribution lines, communications networks to further integrate parts of the electricity grid with control centers, and computerized control devices to automate system management and recovery.

---

## Smart Grid

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 to upgrade their electricity systems, industry and government stakeholders have begun to articulate a broader, more integrated vision for transforming today’s 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 electricity costs.

---

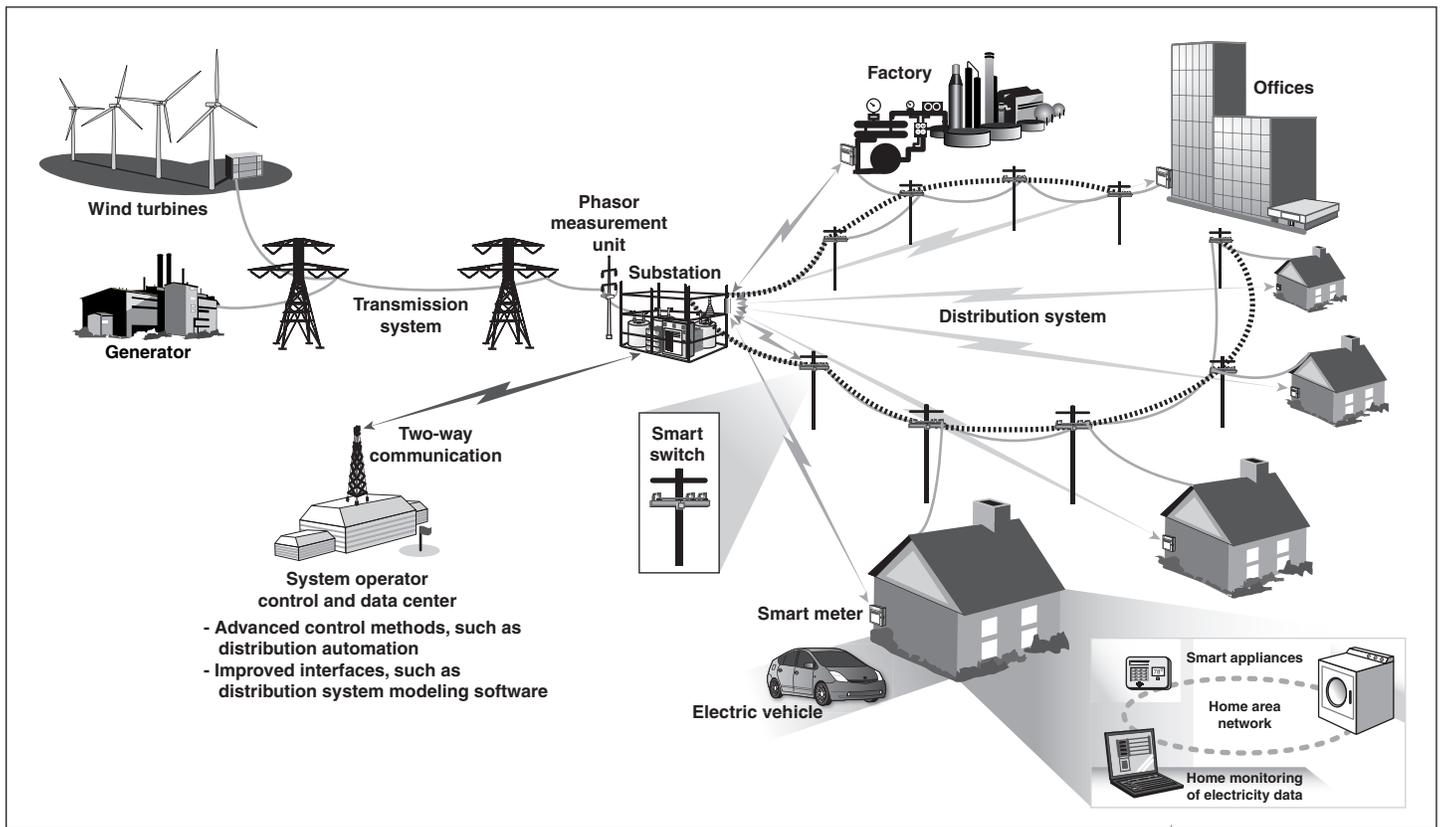
<sup>2</sup>Circuit breakers are devices used to open or close electric circuits. If a transmission or distribution line is in trouble, a circuit breaker can disconnect it from the rest of the system.

<sup>3</sup>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.)

---

This vision—commonly referred to as 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. These efforts are designed to, among other things, improve transmission of electricity from power plants to consumers, provide grid operators with more information about conditions on the electricity system, integrate new and improved technologies into the grid, and allow consumers to receive more information about electricity prices and availability from the electricity system. 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 the customer. For example, FERC estimated advanced metering use in the United States at 4.7 percent in 2008, compared to 0.7 percent in 2006. Initiatives have also involved 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 (called wide-area situational awareness). These include advanced, “smart” switches on the distribution system that communicate with each other to reroute electricity around a troubled line; and high-resolution, time synchronized monitors—called phasor measurement units—on the transmission system. Figure 2 illustrates one possible smart grid configuration. Utilities making actual smart grid investments may choose alternative configurations using different technologies and communications media depending on factors such as cost, customer needs, and local conditions.

**Figure 2: Common Smart Grid Components**



Source: GAO analysis.

Future smart grid applications may also include key roles for energy storage, in particular, storing electricity that is generated when it is inexpensive to produce. This may involve using improved battery technology, including the batteries in plug-in electric and hybrid-electric vehicles. Furthermore, smart grid systems may be used to encourage consumers to lower their demand for electricity during periods of high usage—called peaks. This could occur using home networks that automatically control appliances’ electricity consumption in response to

programmed consumer preferences and information about prices and demand received from the utility.<sup>4</sup>

According to the National Energy Technology Laboratory, a Department of Energy (DOE) national laboratory with a key role in supporting DOE smart grid efforts, smart grid systems fall into several different categories, as outlined in table 1.

**Table 1: Categories of Smart Grid Systems as Defined by the National Energy Technology Laboratory**

System category	Definition	Examples of related smart grid devices
Integrated communications	High-speed, fully integrated, two-way communication technologies that make the smart grid a dynamic, interactive “mega-infrastructure” for real-time information and power exchange. An open architecture facilitates an environment in which technologies from multiple vendors can easily interact and that securely connects grid components, customers, and operators, enabling them to talk, listen, and interact.	<ul style="list-style-type: none"> <li>• Broadband over power line communications technologies</li> <li>• Wireless communications technologies such as WiFi</li> <li>• Home Area Networks—networks of appliances and other devices in the home</li> </ul>
Advanced components	Advanced components that play an active role in determining the electrical behavior of the grid. These power system devices apply the latest research in materials, superconductivity, energy storage, power electronics, and microelectronics to produce higher power densities, greater reliability and power quality, enhanced electrical efficiency that produces major environmental gains, and improved real-time diagnostics.	<ul style="list-style-type: none"> <li>• Advanced or “smart” switches, transformers, cables, and other electrical devices</li> <li>• Storage devices, including plug-in hybrid electric vehicles, as well as advanced batteries</li> <li>• Grid-friendly, “smart” appliances, including air conditioners, clothes washers and dryers, and hot water heaters capable of delaying operation in response to price signals</li> <li>• Microgrids—local electricity grids that can operate independently of the main electricity grid when needed</li> </ul>

<sup>4</sup>We reported in 2004 that demand response—allowing customers to better understand market conditions, such as the price of electricity or limitations in supply, and respond by changing their demand for electricity—has a number of benefits. In particular, demand response programs can enhance reliability and lessen the likelihood of electricity disruptions, such as blackouts. However, our 2004 report found that, at the time, most customers lacked the necessary equipment—meters, communication devices, and special tools—for participating in demand response programs. GAO, *Electricity Markets: Consumers Could Benefit from Demand Programs, but Challenges Remain*, [GAO-04-844](#). (Washington, D.C.: Aug. 13, 2004).

<b>System category</b>	<b>Definition</b>	<b>Examples of related smart grid devices</b>
Advanced control methods	New methods and algorithms that monitor power system components, enabling rapid diagnosis and timely, appropriate response to any event. Integrating this information into planning models could improve utilization of generation and transmission assets.	<ul style="list-style-type: none"> <li>• Substation and distribution automation—real-time monitoring and control of substation and distribution equipment</li> <li>• Fault locator systems that use sensors and digital information to locate faults—failures or drastic changes in current flow or total interruption of an electrical circuit</li> </ul>
Sensing and measurement	Technologies that enhance power system measurements and enable the transformation of data into information. These technologies evaluate the health of equipment and the integrity of the grid, among other things. Such information enables consumers to make choices about whether to use electricity in response to information about electricity prices and demand, and can help provide relief when transmission lines are operating at or near capacity.	<ul style="list-style-type: none"> <li>• Advanced sensors</li> <li>• Advanced metering infrastructure, including “smart” meters</li> <li>• Phasor measurement units—monitors that sample voltage and current many times a second at a given location on the electricity grid to indicate grid stress and trigger corrective actions to maintain reliability</li> <li>• Dynamic line-rating devices that determine the real-time capacity of electrical lines</li> <li>• Consumer portals that provide consumers with real-time information about energy consumption and prices</li> </ul>
Improved interfaces and decision support	Decision support and improved interfaces that will enable more accurate and timely human decision making at all levels of the grid, including the consumer level, while also enabling more advanced operator training.	<ul style="list-style-type: none"> <li>• Software tools to analyze the health of the electricity system</li> <li>• Distribution system modeling software</li> <li>• Real-time digital simulators to study and test electricity systems</li> <li>• Geographic information systems</li> </ul>

Source: National Energy Technology Laboratory, A Compendium of Smart Grid Technologies. July 2009.

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 due to the ability to shift peak demand, an improved ability to transmit power from alternative energy sources such as wind, and an improved ability to detect and respond to potential attacks on the grid. It could also help consumers make more informed choices about when to use electricity; for example, how much to use when demand and prices are high. On the other hand, upgrading the grid would require major investments whose costs would ultimately be passed to utility consumers. Some electricity stakeholders, particularly those representing consumers, question whether the benefits of smart grid investments would be fully realized and have suggested that less costly approaches could achieve similar benefits.

---

State utility regulators are to evaluate applications for smart grid investments on a case-by-case basis. A number of these regulators have approved specific smart grid investments after determining that their benefits to consumers outweigh their costs.

According to the FERC-proposed smart grid policy statement, to achieve the smart grid characteristics and functions outlined in EISA, it is essential that these systems be interoperable—able to work with each other without special effort on the part of the customer. NIST officials explained that the electricity grid has historically relied on proprietary technology which is difficult to integrate with the technology of other manufacturers. In the case of smart grid upgrades, utilities have sought devices and systems that are interoperable and easily integrated with technologies from different vendors.

---

## Smart Grid Cybersecurity

The smart grid vision and its increased reliance on IT systems and networks expose the electric grid to potential and known cybersecurity vulnerabilities associated with using such systems, which in turn increase the risk to the smooth and reliable operation of the electricity grid. As we and others have previously reported,<sup>5</sup> these potential vulnerabilities include:

- increasing the use of systems and networks increases the number of entry points and paths that can be exploited by potential adversaries and other unauthorized users;
- increasing the use of new system and network technologies can introduce new, unknown vulnerabilities;
- interconnecting systems and networks can allow adversaries wider access and the ability to spread malicious activity; and
- increasing the amount of customer information being collected on systems (and transmitting it via networks) provides monetary incentive for adversaries to attack these systems, and could lead to the unauthorized disclosure and use of private information.

---

<sup>5</sup>See, for example, [GAO-07-1036](#).

---

In addition to these potential vulnerabilities, 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, and the impact of such attacks includes the ability to disrupt the electricity grid. In addition, we reported in 2007 that certain smart systems—commonly referred to as control systems—used in industrial settings such as electric generation have cybersecurity vulnerabilities that, if exploited, could result in serious damages and disruption.<sup>6</sup> Further, in 2009, the Department of Homeland Security, in cooperation with a DOE national laboratory, 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.<sup>7</sup>

---

## Smart Grid Regulation

Both the federal government and state governments have authority for overseeing the electricity industry. With respect to the electricity prices and rates of investor-owned utilities, wholesale electricity sales and transmission of electricity in interstate commerce are regulated by the federal government, specifically FERC.<sup>8</sup> This involves approving whether to allow utilities to recover the costs of investments they make to the transmission system. State public utility commissions (PUC) generally have authority to regulate local distribution and retail sales of electricity by investor-owned utilities in their state, including whether to allow these utilities to recover the costs of investments made to the distribution system. For cooperative and some municipal utilities, whose rate regulation by FERC and many state public utility commissions is limited, municipal city councils or cooperative boards of directors will generally

---

<sup>6</sup>[GAO-07-1036](#).

<sup>7</sup>The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C., May 29, 2009).

<sup>8</sup>FERC has the obligation to ensure that the rates charged for wholesale sales of electricity (sales of electricity for resale) by public utilities are just and reasonable and not “unduly discriminatory or preferential.” See 16 U.S.C. §§ 824d, 824e. FERC is composed of up to five commissioners—including one who serves as Chairman—appointed by the President of the United States with the advice and consent of the Senate. Commissioners serve 5-year terms, and have an equal vote on regulatory matters.

---

approve cost recovery for electric investments. With respect to smart grid initiatives, individual utilities can choose to invest in smart grid devices on their own. However, as noted above, depending on the type of utility and where cost recovery is sought, either FERC, the state PUC, or another entity will have authority for deciding whether to allow that utility to recover the costs of smart grid investments from customers.

State and federal authorities also play key roles with respect to reliability, which can be affected by a system's cybersecurity. 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 overseen by FERC. NERC has responsibility for conducting reliability assessments and enforcing mandatory standards to ensure the reliability of the bulk power system—a term that refers to facilities and control systems necessary for operating the electric transmission network and certain generation facilities needed for reliability. NERC develops reliability standards collaboratively through a deliberative process involving utilities and others in the electricity industry—which are then sent to FERC for approval.<sup>9</sup>

These reliability standards include critical infrastructure protection standards for protecting electric utility-critical and cyber-critical assets. In 2008, FERC approved eight critical infrastructure standards developed by NERC. These standards established requirements to help ensure the secure electronic exchange of information needed to operate and support the reliability of the bulk power system, and to help prevent unauthorized physical or electronic access to critical cyber assets. The eight standards require certain users, owners, and operators of the bulk power system to establish policies, plans, and procedures to safeguard physical and electronic access to control systems; identify and protect critical cyber assets; train personnel on security matters; report security incidents; and be prepared to recover from a cyber incident. NERC staff is engaged in the NIST-facilitated process, in particular, to address whether new or modified reliability standards will be necessary to ensure the continued reliability of the bulk power system as new smart grid technologies and systems are developed and integrated with existing systems and networks.

---

<sup>9</sup>Prior to submission to FERC for approval, NERC standards are reviewed and voted on by members of the electricity industry who participate in NERC's FERC-approved standards development process. These standards become mandatory and enforceable in the continental United States only after they are approved by FERC. Once mandatory, both NERC and FERC have authority to enforce reliability standards.

---

## Recent Federal Smart Grid Activities

In 2007, EISA established that it is federal policy to support the modernization of the electricity grid and required actions by a number of federal agencies, including NIST, FERC, and DOE.<sup>10</sup> Specifically, the act directed NIST's Director, who reports to the Secretary of Commerce, to coordinate development of a framework of, among other things, IT standards for achieving the interoperability of smart grid systems. To accomplish this, NIST, starting in 2009, facilitated a process with stakeholders (e.g., utilities, smart grid technology vendors, standards development organizations, and others) to identify interoperability and cybersecurity standards related to smart grid. In January 2010, NIST reported that this process resulted in the identification of 75 standards that support smart grid interoperability. Of these, 11 involved cybersecurity.<sup>11</sup>

In addition to the NIST efforts to develop a framework for identifying interoperability and cybersecurity standards, the agency also identified the need to institute an initiative to develop cybersecurity guidelines for organizations such as electric companies, IT system vendors, and others involved in developing and implementing smart grid systems.

To carry out the above tasks (i.e., developing the standards framework and drafting the cybersecurity guidelines), NIST planned to establish two key working groups that are described in table 2.

---

**Table 2: Key NIST Smart Grid Working Groups**

Group name	Description
Smart Grid Interoperability Panel	<p>A public-private partnership—which was initiated by NIST in 2009—to carry out a variety of tasks related to the development of a smart grid framework for interoperability and cybersecurity standards. This included</p> <ul style="list-style-type: none"><li>• prioritizing and coordinating smart grid standards developed by stakeholders in the NIST process; and</li><li>• administering priority action plans that identify where a new standard or extension of a standard is needed.</li></ul>

---

<sup>10</sup>Pub. L. No. 110-140, (Dec. 19, 2007).

<sup>11</sup>NIST Special Publication 1108, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, January 2010.

Group name	Description
Smart Grid Cyber Security Working Group	<p>A permanent working group of the Smart Grid Interoperability Panel that is to provide expertise needed to address matters related to smart grid cybersecurity. Among other things, this group is to be responsible for</p> <ul style="list-style-type: none"> <li>• developing smart grid cybersecurity guidelines; and</li> <li>• determining if the NIST-identified smart grid standards adequately address cybersecurity, including aligning with these guidelines.</li> </ul>

Source: GAO analysis of NIST documents.

With regard to FERC, under EISA the commission is to adopt those standards (identified as part of the NIST efforts) that it deemed necessary to ensure smart grid systems operate as intended. The act calls for FERC to institute a rule-making proceeding to accomplish this.<sup>12</sup>

Further, with regard to DOE, EISA authorized the department to establish two initiatives to facilitate development of industry smart grid efforts—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)<sup>13</sup> funds available for these respective initiatives. In October 2009, under the Smart Grid Investment Grant Program, DOE announced awards for 100 grants to utilities in multiple states to stimulate the rapid deployment and integration of advanced digital technology needed to modernize the nation’s electric grid. In November 2009, under DOE’s Smart Grid Regional Demonstration Initiative, the department announced awards for 32 grants 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.

In addition to these recent actions, the federal government has undertaken other initiatives to facilitate the implementation of industry smart grid efforts, including funding technical research and development, data

<sup>12</sup>Specifically, EISA allows FERC to adopt any standards necessary for smart grid functionality and interoperability in interstate transmission and regional and wholesale markets. According to FERC officials, if necessary, these standards may affect facilities used at the distribution level, such as smart meters, although EISA does not explicitly limit state authority over local distribution or retail sales.

<sup>13</sup>Pub. L. No. 111-5. (Feb. 17, 2009).

---

collection, and coordination activities (for more details on these efforts see appendix III). Most of these initiatives have been led by DOE.

---

## NIST Has Developed and Issued Smart Grid Cybersecurity Guidelines, but They Do Not Address Some Key Cybersecurity Elements

NIST developed, and issued in August 2010, a first version of its smart grid cybersecurity guidelines. To do this, NIST established in March 2009, the smart grid cyber security working group<sup>14</sup> to, among other things, develop guidelines for entities (e.g., utilities, equipment manufacturers, and regulators) to secure their smart grid systems. NIST intended the guidelines to, among other things, provide a process for entities to follow for developing solutions to address the security of their smart grid systems. To develop the guidelines, NIST planned to have the working group perform an assessment of the cybersecurity risks associated with existing and planned smart grid systems and then use the risk information, and an assessment of the privacy implications of these systems, to identify security requirements (i.e., controls) essential to securing such systems. As part of this assessment, NIST planned to address other key elements of cybersecurity, including the impact of coordinated cyber-physical attacks,<sup>15</sup> and identifying smart grid system vulnerabilities. The working group intended to complete these efforts and issue the guidelines in June 2010.

The working group has largely completed these steps, including issuing the guidelines. Specifically, during 2009 and 2010, the working group defined and then performed a high-level risk assessment of existing and planned smart grid systems—such as for transporting and storing electricity, and for advanced metering infrastructure. The risk assessment included identifying assets, vulnerabilities, and threats as well as specifying impacts for these and other systems as a means to identify security requirements (i.e., controls)—such as access control policies and procedures, employee training programs, incident response, and risk management—for securing such systems.

---

<sup>14</sup>In March 2009, NIST established this group, calling it the Cyber Security Coordination Task Group. In January 2010, NIST renamed it the Smart Grid Cyber Security Working Group. The working group is comprised of about 400 participants from the electricity industry, including electric companies, IT system vendors, smart grid system vendors, service providers, federal and state regulatory organizations, and academia.

<sup>15</sup>A coordinated cyber-physical attack involves using both cyber and physical means to attack a target. For example, a cyber attack could be aimed at disabling a security system in order to facilitate a physical attack (e.g., damaging electric grid components) against a utility's infrastructure.

---

Using the results of the risk assessment and other efforts, the working group issued the smart grid cybersecurity guidelines in August 2010.<sup>16</sup> The guidelines include important elements, such as a high-level strategy that organizations can use to develop an approach to securing their smart grid systems, including identifying appropriate security requirements. In addition, the guidelines

- identified potential cryptography<sup>17</sup> issues that entities may encounter and solutions for resolving these issues;
- included a privacy impact assessment for the smart grid with a discussion of mitigating factors;
- identified potential smart grid vulnerabilities, as well as the possible impacts to organizations should the vulnerabilities be exploited;
- identified smart grid security problems, including how to ensure that access can be gained to critical devices and systems by personnel when ordinary authentication fails for any reason, and how to ensure that updates utilities send to smart meters are secure;
- detailed cybersecurity design issues, such as for password complexity rules; and
- identified smart grid cybersecurity areas requiring further research and development.

NIST stated in the guidelines that this initial version was to be updated periodically to incorporate any emerging issues.

While NIST largely addressed the key elements in developing its guidelines, it did not address an important element essential to securing smart grid systems and networks that NIST had planned to include. Specifically, it did not address the risk of combined cyber-physical attacks.

---

<sup>16</sup>NIST Interagency Report 7628, *Guidelines for Smart Grid Cyber Security*, August 2010.

<sup>17</sup>Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. One such mechanism is encryption. Encryption can be used to provide basic confidentiality and integrity of transmitted or stored data by transforming plain text into cipher text using a special value, known as a key, and a mathematical process, known as an algorithm.

---

NIST also identified other key elements that surfaced during its development of the guidelines that need to be addressed in future guideline updates. These include identifying

- research and development that needs to be performed, such as for synchrophasor<sup>18</sup> security;
- cryptography issues, and solutions to resolve cryptography issues; and
- additional smart grid system design issues, such as managing vulnerabilities incurred in the supply chain.

NIST officials said they did not address the cyber-physical and other above topics in the guidelines because, in part, they had not yet fully developed these sections by the planned June 2010 issuance date. Consequently, if NIST had taken the time to address and incorporate these topics, it would have caused the agency to have been even further behind schedule, meaning the guidelines would have been issued later than August 2010.

NIST officials also said that the working group intends to update the guidelines to, among other things, address these missing elements. To do so, NIST drafted a plan and schedule for updating the cybersecurity guidelines periodically. While a positive step, the plan and schedule, as of October 2010, were still in draft form. NIST officials stated that they are in the process of rewriting the plan and schedule and intend to have them finalized by the end of the year.

Having a finalized plan and schedule with specific milestones is critical for ensuring the guidelines fully address key cybersecurity elements that have not been incorporated thus far. Without it, there is increased risk that important cybersecurity elements will not be addressed by entities implementing smart grid systems, thus making these systems vulnerable to attack.

---

<sup>18</sup>Synchrophasor systems provide detailed data on the conditions of the transmission and distribution grid, which is used to improve power system reliability.

---

## FERC Has Begun Reviewing Initial Smart Grid Standards but Has Not Developed a Coordinated Plan to Monitor Industry's Implementation

In 2010, FERC began reviewing for adoption an initial set of smart grid interoperability and cybersecurity standards developed through the NIST standards process. However, FERC has not developed a coordinated approach with other regulators to monitor the extent to which industry follows these voluntary standards, because, according to officials, it has not yet determined whether or how to perform such a task. Without a documented approach to coordinate with state and other regulators on this issue, FERC will not be well positioned to promptly begin monitoring the results of any standards it adopts or quickly respond if gaps arise.

---

## FERC Has Begun Reviewing an Initial Set of Smart Grid Standards, but Enforcement Authorities Are Divided Among Multiple Regulators

In October 2010, FERC began its process of reviewing for adoption smart grid standards related to interoperability and cybersecurity, but authority to enforce these standards is divided among multiple regulators. The five standards being initially reviewed were identified by NIST as ready for regulator consideration and represent a subset of those identified through the NIST-facilitated smart grid standards process.<sup>19</sup> FERC designated a docket for a proceeding to review these five standards and adopt those that it believes are necessary to ensure smart grid functionality and interoperability in interstate transmission of electric power and regional and wholesale electricity markets. FERC staff were uncertain when the initial set of standards would be adopted, but both FERC and NIST officials told us that, because smart grid standards are continually evolving, they expect multiple rounds of standards to be reviewed and adopted by FERC. FERC staff have suggested various criteria that they believe the Commissioners should use when considering whether to adopt the standards, including recommending relying on the assessment of the NIST Cyber Security Working Group and rule making comments to determine if cybersecurity has been adequately incorporated. FERC also provided guidance to help NIST prioritize interoperability standards development. In a July 2009 smart grid policy statement, FERC proposed prioritizing two crosscutting issues—system security (including cybersecurity) and intersystem communication—along with four key

---

<sup>19</sup>NIST facilitated a process of stakeholder identification of standards to promote smart grid interoperability and cybersecurity. NIST's Cyber Security Working Group plans to evaluate whether these smart grid standards adequately address cybersecurity, including whether they align with the guidelines discussed in the previous section.

---

functionalities—wide area situational awareness,<sup>20</sup> demand response, electric storage, and electric transportation.

While EISA gives FERC authority to adopt smart grid standards, it does not provide FERC with specific enforcement authority. In particular, EISA gives FERC the authority to adopt standards once it finds the NIST process has led to sufficient consensus. 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. Stakeholders we spoke with—federal electricity officials, participants in the smart grid standards development process, and other electricity and cybersecurity experts—noted that, while voluntary industry-developed standards have historically been used in the electricity industry, some factors could limit the extent to which they are followed. Although some explained that economic and market pressure should encourage manufacturers and utilities to follow voluntary standards, others noted that there could still be gaps in the extent to which the standards are followed, particularly if the cost of following standards is high or if utilities have varying levels of familiarity with and interest in implementing them.

According to FERC officials, FERC’s only authority to require utilities to follow standards or use standards-compliant devices would derive from its existing reliability and cost-recovery authorities under the Federal Power Act, which generally apply to transmission assets.<sup>21</sup> For example, FERC could require that utilities subject to its rate regulation use standards-compliant smart grid devices as a condition of allowing them to recover the costs of smart grid investments on the transmission system. Additionally, to the extent that interoperability and cybersecurity standards are deemed necessary to ensure the reliability of the bulk power

---

<sup>20</sup>Wide-area situational awareness is the visual display of broad electricity system conditions in near real time.

<sup>21</sup>According to FERC, its cost recovery authority for electricity investments extends to facilities used for transmission in interstate commerce. Its reliability authority applies to the bulk power system—a term that refers to facilities and control systems necessary for operating the electric transmission network and certain generation facilities needed for reliability. FERC also has regulatory authority over most of the interstate wholesale market in electricity. However, it is unclear how this authority applies to enforcement of smart grid interoperability and cybersecurity standards.

---

system, such standards could be considered through the NERC standards-setting process, and if approved, would be considered mandatory and enforceable by both NERC and FERC. However, FERC officials noted that NERC's reliability standards-setting process involves extensive deliberation by industry; that it is possible that NERC could choose not to develop a mandatory reliability standard that FERC had adopted through its separate process for smart grid standards; and that FERC is prohibited from adopting reliability standards on its own outside of the NERC process.

The fragmented nature of electricity industry regulation further complicates enforcement of smart grid standards and oversight of smart grid investments using FERC and other regulators' existing authorities.<sup>22</sup> Oversight responsibility is divided among various regulators at the federal, state, and local level, and FERC's authority is limited to certain parts of the grid, generally the transmission system. As a result, state regulatory bodies and other regulators with authority over the distribution system will play a key role in overseeing the extent to which interoperability and cybersecurity standards are followed since many smart grid upgrades will be installed on the distribution system. Such regulatory fragmentation can make it difficult for individual regulators to develop an industry-wide understanding of whether utilities and manufacturers are following voluntary standards. This is due to the large number of regulators in the industry—FERC, electricity regulators in 50 states and the District of Columbia, and regulators of thousands of cooperative and municipal utilities—and their potentially limited visibility over parts of the grid outside their jurisdiction.

The state public utility commissions we spoke with were at different points in developing their approach to monitoring smart grid

---

<sup>22</sup>Past GAO work discusses divided regulatory responsibilities in the electricity industry. GAO, *Electricity Restructuring: Key Challenges Remain*, [GAO-06-237](#) (Washington, D.C.: Nov. 15, 2005), GAO, *Electricity Markets: FERC's Role in Protecting Consumers*, [GAO-03-726R](#) (Washington, D.C.: June 6, 2003), GAO, *Electricity Restructuring: 2003 Blackout Identifies Crisis and Opportunity for the Electricity Sector*, [GAO-04-204](#) (Washington, D.C.: Nov. 18, 2003), GAO, *Electricity Restructuring: Action Needed to Address Emerging Gaps in Federal Information Collection*, [GAO-03-586](#) (Washington, D.C.: June 30, 2003). Additional past GAO reports can be found at the end of this report.

---

interoperability and cybersecurity.<sup>23</sup> Multiple state regulators told us that, while they have not imposed any formal requirements on utilities with respect to the interoperability and cybersecurity of smart grid technologies, their offices have ongoing conversations with regulated utilities about the issue. Others have established requirements in PUC rule makings outlining minimum functionalities that smart meters must achieve, and in the case of the Public Utility Commission of Texas, audits that smart meter manufacturers must obtain to demonstrate that smart meter data can be securely accessed by customers and others. Additionally, the California and Colorado commissions have opened proceedings to initiate discussion with the public about how to best address topics like the interoperability and cybersecurity of smart grid technologies. Finally, most PUC staff were uncertain what approach their Commissions would take to enforce any standards that FERC decides to adopt, and three said that limited resources and technical expertise made their roles in overseeing interoperability and cybersecurity, including participating in the NIST standards process, more challenging.

A number of cooperatively and municipally owned utilities fall partially out of the purview of federal and state regulators, and as such, it will be up to their regulators—often utility boards of directors—to oversee the interoperability and cybersecurity of their smart grid efforts. In Nebraska, for example, the state is entirely composed of consumer owned utilities, including municipal and cooperative utilities and public power districts. This means that, in part, oversight of smart grid interoperability and cybersecurity in this state will fall to the numerous individual regulators of these utilities. In addition, there are thousands of cooperatively and municipally owned utilities located across the country.

---

<sup>23</sup>In one of the seven states in which we spoke with electricity regulators, the state electricity regulators did not have authority to oversee whether smart grid investments are interoperable and cyber secure. The Nebraska Power Review Board and Nebraska Public Service Commission are the primary agencies in Nebraska charged with regulating electricity. However, all utilities in Nebraska are consumer owned—such as cooperative or municipal utilities and public power districts, and neither regulator has authority to oversee whether smart grid investments are interoperable or cyber secure.

---

## FERC Has Not Developed a Coordinated Approach to Monitor Whether Industry Follows Voluntary Standards

Despite the importance of ensuring manufacturers and utilities follow smart grid standards, FERC has 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 have been some initial efforts by regulators to share views. For example, a collaborative dialogue between FERC and the National Association of Regulatory Utility Commissioners (NARUC) to facilitate the transition to a smart electric grid—the FERC-NARUC Collaborative on Smart Response—has discussed the standards-setting process in general terms. However, according to FERC and NARUC officials, FERC and the state PUCs have 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. According to FERC officials and others representing municipal and cooperative utilities, FERC also has not coordinated in such a way with groups representing public power and cooperative utilities—utilities not routinely subject to FERC’s or the states’ jurisdiction for rate-setting purposes. Such groups include the American Public Power Association, which represents municipally owned utilities, and the National Rural Electric Cooperative Association, which represents cooperatively owned utilities. FERC has not developed such an approach, because, according to officials, it has not yet determined whether or how to conduct high-level monitoring of compliance with smart grid standards it adopts under EISA.

Adherence to standards is an important step toward achieving an interoperable and secure electricity system. Unless FERC and other regulators have a good understanding of whether utilities and manufacturers are following smart grid standards, it will be difficult to know whether a voluntary approach to standards setting is effective or if changes are needed. According to federal internal control guidance, managers need to compare actual performance—in this case, the extent to which manufacturers and utilities follow voluntary standards—to planned or expected results throughout the organization and analyze significant differences.<sup>24</sup> Given the fragmented nature of electricity regulation, it may not be possible for FERC to perform such a review alone, and the agency may have to collaborate with other regulators. Past GAO work highlights that when carrying out activities to enhance interagency collaboration, it is critical to involve nonfederal partners—in this case, state and other

---

<sup>24</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington D.C.: November 1999).

---

regulators with responsibility for overseeing key components of the electricity industry—in decision making.<sup>25</sup> Without a documented approach established in advance to coordinate with state and other regulators on this issue, FERC will not be well positioned to promptly begin monitoring the results of any standards it adopts—including a high-level assessment of whether industry follows them—and quickly respond if gaps arise. Such a delay could result in a patchwork of approaches across the United States and lead to incompatibilities between systems, higher costs, and a less secure electricity grid.

A number of activities are under way that may result in information to inform a FERC assessment of the extent to which voluntary standards are followed, but these efforts are not coordinated or complete. According to DOE officials, as a part of DOE's broader effort to publish a smart grid system report every 2 years as required by EISA, the department expects to report some information about the progress and effectiveness of smart grid interoperability and cybersecurity standards. Additionally, NIST has efforts under way to establish a process for vendors to certify their smart grid products as complying with standards and coordinate industry development of additional standards as needed. However, it is unclear to what extent these planned activities will specifically focus on assessing industry compliance with voluntary standards across regulatory jurisdictions and options to address any gaps that exist. Moreover, unlike FERC, the state PUCs, and other electricity regulators, neither DOE nor NIST has the authority to routinely require industry to follow standards should gaps exist.

---

## Electricity Industry Faces Key Challenges to Securing Smart Grid Systems and Networks

Leveraging the views of experts (by means of panel discussions), we identified the following six challenges that are key to ensuring the cybersecurity of the systems and networks that support our nation's electricity grid.

- *Aspects of the current regulatory environment make it difficult to ensure the cybersecurity of smart grid systems.* In particular, jurisdictional issues and the difficulties associated with responding to continually evolving cyber threats are a key regulatory challenge to ensuring the cybersecurity of smart grid systems as they are deployed. Regarding

---

<sup>25</sup>GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies* [GAO-06-15](#) (Washington D.C.: October 2005).

---

jurisdiction, our experts 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 technology is located on the transmission or distribution system, experts raised concerns that smart grid technology may blur these lines. For example, devices such as smart meters deployed on parts of the grid traditionally subject to state jurisdiction could, in the aggregate, have an impact on those parts of the grid that federal regulators are responsible for—namely the reliability of the transmission system.

There is also concern about the ability of regulatory bodies to respond to evolving cybersecurity threats. For example, one expert questioned the ability of government agencies to adapt to rapidly evolving threats, while another highlighted the need for regulations to be capable of responding to the evolving cybersecurity issues. In addition, our experts expressed concern with agencies developing regulations in the future that are overly specific in their requirements, such as those specifying the use of a particular product or technology. Consequently, unless steps are taken to mitigate these challenges, regulations may not be fully effective in protecting smart grid technology from cybersecurity threats.

- *Consumers are not adequately informed about the benefits, costs, and risks associated with smart grid systems.* Specifically, there is concern that consumers are not aware of the benefits, costs, and risks associated with smart grid systems. This lack of awareness may limit the extent to which consumers are willing to pay for secure and reliable systems, which may cause regulators to be reluctant to approve rate increases associated with cybersecurity. As a result, until consumers are more informed about the benefits, costs, and risks of smart grid systems, utilities may not invest in, or get approval for, comprehensive security for smart grid systems, which may increase the risk of attacks succeeding.
- *Utilities are focusing on regulatory compliance instead of comprehensive security.* The existing federal and state regulatory environment creates a culture within the utility industry of focusing on compliance with cybersecurity requirements, instead of a culture focused on achieving comprehensive and effective cybersecurity. Specifically, experts told us that utilities focus on achieving minimum regulatory requirements rather than designing a comprehensive approach to system security. In addition, one expert stated that security requirements are inherently incomplete, and having a culture that views the security problem as being solved once those requirements are met will leave an

---

organization vulnerable to cyber attack. Consequently, without a comprehensive approach to security, utilities leave themselves open to unnecessary risk.

- *There is a lack of security features being built into smart grid systems.* Security features are not consistently built into smart grid devices. For example, our experts told us that certain currently available smart meters have not been designed with a strong security architecture and lack important security features, including event logging<sup>26</sup> and forensics capabilities which are needed to detect and analyze attacks. In addition, our experts stated that smart grid home area networks—used for managing the electricity usage of appliances and other devices in the home—do not have adequate security built in, thus increasing their vulnerability to attack. Without securely designed smart grid systems, utilities will be at risk of not having the capacity to detect and analyze attacks, which increases the risk that attacks will succeed and utilities will be unable to prevent them from recurring.
- *The electricity industry does not have an effective mechanism for sharing information on cybersecurity and other issues.* The electricity industry lacks an effective mechanism to disclose information about smart grid cybersecurity vulnerabilities, incidents, threats, lessons learned, and best practices in the industry. For example, our experts stated that while the electricity industry has an information sharing center, it does not fully address these information needs. In addition, President Obama’s cyberspace policy review, released in May 2009, also identified challenges related to cybersecurity information sharing within the electric and other critical infrastructure sectors and issued recommendations to address the areas.<sup>27</sup> According to our experts, information regarding incidents such as both unsuccessful and successful attacks must be able to be shared in a safe and secure way 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 cyber attacks and their methods, which could help grid operators better defend against them. If the industry pursued this end, it could draw upon the practices and

---

<sup>26</sup>Event logging is a capability of an IT system to record events occurring within an organization’s systems and networks, including those related to computer security.

<sup>27</sup>The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C., May 29, 2009).

---

approaches of other industries when designing an industry-led approach to cybersecurity information sharing. Without quality processes for information sharing, utilities will not have the information needed to adequately protect their assets against attackers.

- *The electricity industry does not have metrics for evaluating cybersecurity.* The electricity industry is 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<sup>28</sup> are difficult to develop, they could help compare the effectiveness of competing solutions and determine what mix of solutions combine to make the most secure system. Furthermore, our experts said 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, 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 investments.

---

## Conclusions

The electricity industry is in the midst of a major transformation as a result of smart grid initiatives, and this transformation has led to significant financial investment by many entities, including utilities, private companies, and the federal government. For their part, NIST and FERC have efforts planned and under way to carry out their smart grid roles and responsibilities, although limitations exist in the planning and coordination efforts of these two key agencies. Specifically, NIST does not have a definitive plan and schedule, including specific milestones, for updating and maintaining its cybersecurity guidelines to address key missing elements. Furthermore, FERC has not established an approach coordinated with other regulators to monitor the extent to which industry is following the smart grid standards it adopts.

The voluntary standards and guidelines developed through the NIST and FERC processes offer promise. However, a voluntary approach poses some risks when applied to smart grid investments, particularly given the fragmented nature of regulatory authority over the electricity industry. Currently, NIST and FERC's efforts are hindered by their lack of an

---

<sup>28</sup>Metrics can be used for, among other things, measuring the effectiveness of cybersecurity controls for detecting and blocking cyber attacks.

---

approach to (1) updating voluntary cybersecurity guidelines and (2) monitoring whether voluntary standards are being followed by manufacturers and utilities and periodically reporting to Congress on whether additional authorities are needed. Not having such an approach could result in gaps being recognized too late to avoid incompatibilities between systems, costly equipment replacements, or unnecessarily long periods of vulnerability to cyber attack. The lack of an approach to monitoring compliance with standards also limits the information available to Congress on how widely the smart grid standards are being followed and whether additional regulatory authorities are needed to address any gaps.

In addition to the challenges being faced by NIST and FERC, the electricity industry faces its own set of challenges that are critical to ensuring smart grid systems and networks are implemented securely. Addressing these challenges will involve participation by private sector organizations and government agencies, including NIST and FERC. Because these two agencies are key to addressing the challenges, it is especially important that NIST and FERC when addressing their planning and coordination limitations also consider whether the challenges should be addressed in their current and planned cybersecurity efforts.

---

## Recommendations for Executive Action

To reduce the risk that NIST's smart grid cybersecurity guidelines will not be as effective as intended, we recommend that the Secretary of Commerce direct the Director of NIST to finalize the agency's plan for updating and maintaining the cybersecurity guidelines, including ensuring it incorporates (1) missing key elements identified in this report, and (2) specific milestones for when efforts are to be completed. We also recommend that NIST, as a part of finalizing the plan, assess whether any cybersecurity challenges identified in this report should be addressed in the guidelines.

To improve coordination among regulators and help Congress better assess the effectiveness of the voluntary smart grid standards process, we recommend that the Chairman of FERC, making use of existing smart grid information, develop an approach to

- coordinate with state regulators to (1) periodically evaluate the extent to which utilities and manufacturers are following voluntary interoperability and cybersecurity standards and (2) develop strategies for addressing any gaps in compliance with standards that are identified as a result of this evaluation. To the extent that FERC determines it lacks authority to

---

address any gaps in compliance that cannot be addressed through this coordinated approach with other regulators, the Chairman should report this information to Congress.

- coordinate with groups that represent utilities subject to less FERC and state regulation (such as municipal and cooperative utilities) to (1) periodically evaluate the extent to which utilities and manufacturers are following voluntary interoperability and cybersecurity standards and (2) develop strategies for addressing any gaps in compliance with standards that are identified as a result of this evaluation. To the extent that FERC determines it lacks authority to address any gaps in compliance that cannot be addressed through this coordinated approach, the Chairman should report this information to Congress.

We also recommend that the Chairman of FERC, working with NERC as appropriate, assess whether any cybersecurity challenges identified in this report should be addressed in commission cybersecurity efforts.

---

## Agency Comments and Our Evaluation

In written comments—signed by the Secretary of Commerce and the Chairman of FERC (see appendixes IV and V, respectively)—on a draft of this report, both agencies stated that they agreed with our recommendations.

Although Commerce agreed with the recommendations, the department (1) offered three related comments on a finding in the report, and (2) suggested rewording part of our recommendations based on those comments. Specifically, in the first two comments, the department wanted to replace wording we used in the report (i.e., replacing “missing key elements” with “NIST’s follow-on cyber-physical activity”) and delete two report sentences which, in its view, incorrectly implied that NIST planned to complete its cyber-physical activity and report its work results in the issuance of the August 2010 guidelines. In its third comment, Commerce agreed that the risk of combined cyber-physical attacks needs to be addressed in the guidelines, but reiterated its disagreement with our report statement that NIST was planning to cover this in the August 2010 guidelines. Based on these comments, the department suggested wording changes to part of our recommendations to reflect its view. However, our review of drafts of the guidelines, including one issued by NIST to the public in February 2010, coupled with discussions with NIST officials responsible for developing the guidelines, show that that the agency had planned to address this topic in the August 2010 version of the guidelines. Based on this evidence, we did not make any changes to our report.

---

In addition to agreeing to our recommendations, FERC also (1) commended the draft report's discussion of cybersecurity for the electric industry, (2) said it appreciated the report's conclusions, and (3) described steps it intended to take to implement the recommendations. Specifically, with regard to our recommendation to improve coordination among regulators, FERC stated that it intends to direct commission staff to evaluate possible approaches to improving coordination among regulators. In addition, FERC stated that if the commission finds that it lacks authority to address gaps in electric industry compliance with voluntary interoperability and cybersecurity standards, it intends to report this information to Congress as our report recommends. Further, in response to our recommendation to assess whether any of the challenges identified in our report should be addressed in commission cybersecurity efforts, FERC said it had directed commission staff to develop procedures to perform such an assessment.

In addition to the above comments, FERC also presented two general issues with the report. The first is that while FERC agreed with the challenge associated with the lack of cybersecurity metrics, identified in the draft, it commented that developing valid metrics also presents a separate challenge of its own. We agree with this view and believe it is consistent with our report findings. The second issue is that according to FERC, our report appeared to assume that all relevant manufacturers and utilities are to comply with the voluntary standards being developed through the process specified in EISA. To clarify, we neither stated this assumption in our report nor was it our intent to imply such an assumption. Nonetheless, it is important to note that the findings described in our report show it is critical for FERC to determine the extent to which these standards are being followed, and that is why we included a recommendation for the agency to coordinate with state regulators and others to achieve this goal.

We also provided a copy of the draft report for review and comment to DOE. In an e-mail from the Team Lead for Strategic Planning and Daily Operations within DOE's Office of Electricity Delivery and Energy Reliability, the department provided technical comments on the report, which we incorporated as appropriate.

---

We are sending copies of this report to the appropriate congressional committees, Secretary of Commerce, Director of NIST, Chairman of FERC, and other interested parties. The report is also available at no charge on the GAO Web site at <http://www.gao.gov>.

---

If you or your staffs have questions about matters discussed in this report, please contact David Powner at (202) 512-9286 or David Trimble at (202) 512-3841, or by e-mail at [pownerd@gao.gov](mailto:pownerd@gao.gov) or [trimbled@gao.gov](mailto:trimbled@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix VI.



David A. Powner  
Director, Information Technology  
Management Issues



David C. Trimble  
Acting Director, Natural Resources  
and Environment

---

# Appendix I: Objectives, Scope, and Methodology

---

Our objectives were to (1) assess the extent to which the National Institute of Standards and Technology (NIST) has developed smart grid cybersecurity guidelines, (2) evaluate the Federal Energy Regulatory Commission's (FERC) efforts to adopt smart grid cybersecurity and other standards and monitor their use by industry, and (3) identify challenges associated with ensuring the cybersecurity of the smart grid.

For our first objective, we analyzed applicable laws to determine NIST's responsibilities with respect to the smart grid. Then we analyzed agency plans and related documentation and interviewed responsible officials to determine the steps NIST was planning to take or had taken to meet those responsibilities. Specifically, we analyzed NIST's plans for developing smart grid cybersecurity guidelines, and compared them with the issued guidelines<sup>1</sup> to identify any differences. Where there was a difference between NIST's plans and what had been completed, we analyzed the impact of the difference and its cause.

For the second objective, we analyzed FERC documentation, including their interim and final Smart Grid Policy Statement,<sup>2</sup> and reviewed relevant laws and regulations. We interviewed FERC staff to better understand their authority with respect to smart grid standards, expected approach to standards adoption, and the extent of coordination with other regulators. We also interviewed state electricity regulators to understand their regulatory approach and perspectives on smart grid standards being identified and developed through the NIST process. The state regulators we sought the views of included the Alabama Public Service Commission, California Public Utilities Commission, Colorado Public Utilities Commission, Nebraska Power Review Board, Public Utilities Commission of Ohio, Pennsylvania Public Utility Commission, and the Public Utility Commission of Texas. These states were selected because they had smart grid activities of interest and were generally varied in terms of location, size, and regulatory structure. As part of this work, we identified the steps taken by these states to oversee interoperability and cybersecurity of smart grid investments, although we did not evaluate their adequacy. In Nebraska, because all utilities are consumer-owned, state electricity regulators do not have authority to oversee whether smart grid investments are interoperable or cyber secure. As a result, we excluded

---

<sup>1</sup>NIST Interagency Report 7628, *Guidelines for Smart Grid Cyber Security*, August 2010.

<sup>2</sup>FERC, Smart Grid Policy Statement, Docket No. PL09-4-000 (Washington, D.C., July 16, 2009).

Nebraska from any summaries of state responses presented in the body of this report. We also met with staff from two groups representing public and cooperatively owned utilities: the American Public Power Association and the National Rural Electric Cooperative Association. Additionally, we reached out to various electricity experts, including representatives of standards development organizations, participants in the NIST standards development process, and others, to gather their opinions on the strengths and limitations of the NIST approach and standards setting.

For our third objective, we convened a panel of experts in coordination with the National Academy of Sciences. Specifically, we worked iteratively with the National Academy of Sciences' Computer Science and Telecommunication Board to choose a group of panel members with expertise in subjects most applicable to our objective. The selected experts included representatives from electric utilities responsible for implementing and securing smart grid systems, public utility commissions, trade associations, smart grid technology vendors, and cybersecurity experts. A full list of the expert panelists can be found in appendix III. A key topic discussed by the panel was the major cybersecurity challenges facing the grid, and related issues, such as the potential consequences of security failures, adequacy of current cybersecurity technology, effectiveness of regulatory frameworks and enforcement mechanisms, potential benefits for key stakeholder groups, and additional steps regulators could take to ensure that smart grid investments are secure. We then analyzed the results of the panel, and from that analysis developed a list of the major challenges and a summary of each. We then had the panelists review the list and our accompanying summary to make sure we accurately captured their views.

We conducted this performance audit from November 2009 to January 2011, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit 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.

# Appendix II: Other Federal Efforts to Facilitate Smart Grid Implementation

In addition to efforts discussed in this report, the federal government has undertaken other efforts to facilitate smart grid implementation, including conducting and funding technical research and development, data collection, and coordination activities. Most of these initiatives have been led by the Department of Energy (DOE). Table 3 describes 10 of these other key efforts, including the federal agency involved and the purpose of the effort.

**Table 3: Other Federal Efforts to Support Smart Grid Implementation**

<b>Effort</b>	<b>Federal agency that established effort and year</b>	<b>Membership or contractors</b>	<b>Purpose of effort</b>
Smart Grid Cybersecurity Web site	Established by DOE and its Pacific Northwest National Laboratory and launched in January 2010	DOE and Pacific Northwest National Laboratory	To share information about smart grid cybersecurity and cybersecurity approaches used in smart grid demonstration and investment grant projects.
GridWise Architecture Council	Established by DOE in 2004	Recognized practitioners and leaders from the electricity industry and related sectors, including state governments and private representatives, ranging from major corporations to independent systems operators and others	To promote and enable interoperability among the many entities that interact with the nation's electric power system. The council enlists industry involvement to articulate the goal of interoperability across the electric system; identify the concepts and architectures needed to make interoperability possible, and develop actionable steps to facilitate the interoperation of systems, devices, and institutions that encompass the nation's electric system.
Federal Energy Regulatory Commission and National Association of Regulatory Utility Commissioners (FERC-NARUC) Collaborative on Smart Response	The smart grid component of this collaborative was established by FERC and NARUC in 2008	NARUC and FERC	To provide a forum for federal and state regulators to discuss the smart grid and demand response policies, share best practices and technologies, and address issues that benefit from state and federal collaboration.
North American SynchroPhasor Initiative	Established in 2007 by DOE and the North American Electric Reliability Corporation (NERC) along with electric utility companies and other organizations	DOE; NERC; North American electric utilities, vendors, and consultants; federal and private researchers; and academics	To promote power system reliability and visibility through wide-area measurement and control using smart grid synchrophasor technology. Its mission is to encourage a robust, widely available, and secure synchronized data measurement infrastructure for the interconnected North American electric power system with associated analysis and monitoring tools for improved reliability and better planning and operation. This effort builds upon prior related DOE efforts.

**Appendix II: Other Federal Efforts to Facilitate Smart Grid Implementation**

<b>Effort</b>	<b>Federal agency that established effort and year</b>	<b>Membership or contractors</b>	<b>Purpose of effort</b>
Smart Grid Advisory Committee	Established in 2008 by DOE, as required by the Energy Independence and Security Act of 2007 (EISA)	Members are selected by the DOE secretary from both private and nonfederal public sector stakeholders based on their experience, expertise, and ability to represent the full range of smart grid technologies and services	To advise relevant federal officials concerning the development of smart grid technologies, the progress of a national transition to the use of smart grid technologies and services, the evolution of widely accepted technical and practical standards and protocols to allow interoperability and intercommunication among smart grid-capable devices, and the optimum means of using federal funding to encourage such progress. According to DOE officials, the committee was incorporated into the Electricity Advisory Committee.
Smart Grid Data Hub and smartgrid.gov Web site	Initiated by DOE in 2009. DOE contracted with the National Renewable Energy Laboratory to lead multiple labs in developing, establishing, and maintaining the data hub and Web site	DOE, the National Renewable Energy Laboratory, Lawrence Berkeley National Laboratory, Oak Ridge National Laboratory, and Navigant Consulting Inc.	To collect and maintain information about the American Recovery and Reinvestment Act-funded smart grid activities and their progress to help inform and educate consumers about all aspects of the smart grid.
Smart Grid Information Clearinghouse	Initiated by DOE in 2009. DOE contracted with Virginia Tech to design, establish, and initially maintain this clearinghouse	DOE, Virginia Tech, the IEEE Power & Energy Society, and EnerNex	To serve as a repository for government and industry smart grid information including standards, projects, lessons learned, and best practices to facilitate wide-ranging data gathering and information sharing. It is located at <a href="http://www.sgiclearinghouse.org">http://www.sgiclearinghouse.org</a> .
Smart Grid Maturity Model	Originally developed by IBM and seven utilities. In 2009, Carnegie Mellon University's Software Engineering Institute became the steward for this model. DOE sponsors the institute's activities related to the model	DOE and Carnegie Mellon University	To provide a management tool to help utilities assess and improve their progress in implementing the smart grid.

**Appendix II: Other Federal Efforts to Facilitate Smart Grid Implementation**

<b>Effort</b>	<b>Federal agency that established effort and year</b>	<b>Membership or contractors</b>	<b>Purpose of effort</b>
Smart Grid Task Force	Established by DOE in 2008, as required by EISA	Electricity experts from DOE, FERC, the National Institute of Standards and Technology (NIST), and other federal entities (e.g., Environmental Protection Agency, Department of Homeland Security, Department of Agriculture, and Department of Defense)	To ensure awareness, coordination, and integration of federal government activities related to smart grid technologies, practices, and services.
DOE National Laboratory smart grid projects	Initiated over multiple years at various DOE labs	National Laboratories include: <ul style="list-style-type: none"> <li>• Ames,</li> <li>• Argonne,</li> <li>• Lawrence Berkeley,</li> <li>• Idaho,</li> <li>• National Energy Technology Laboratory,</li> <li>• National Renewable Energy Laboratory,</li> <li>• Oak Ridge,</li> <li>• Pacific Northwest National Laboratory, and</li> <li>• Sandia National Laboratories</li> </ul>	To support smart grid development by conducting and funding technical research and development projects, such as modeling; standards development and conformance testing; and development of smart grid devices and applications; among other things. For example, Argonne National Laboratory has a modeling project to analyze the impact of smart grid technologies (e.g., plug-in hybrid electric vehicles—vehicles that interconnect with the grid to charge and store electricity on grid infrastructure, electricity demand, and electricity prices). In addition, in the area of standards development, multiple labs participate in the NIST smart grid standards process. Additionally, several laboratories are developing smart grid devices and applications, such as Sandia, which is developing sensing, monitoring, and control devices to address the technical challenges associated with integrating renewable energy systems into the current transmission and distribution infrastructure.

Source: GAO analysis of agency and industry sources.

---

# Appendix III: Expert Panel Discussion Attendees

---

The names and affiliation of the experts who participated in the panel discussion held June 2-3, 2010, in Washington, D.C., are:

- Sharla Artz, Director of Government Affairs, Schweitzer Engineering Laboratories, Inc.
- David Baker, Director of Services, IOActive, Inc.
- David Batz, Manager, Cyber & Infrastructure Security, Edison Electric Institute
- W. Earl Boebert, Sandia National Laboratories (retired)
- Michael Butler, Senior Analyst, National Institute of Standards and Technology
- Matthew Carpenter, Senior Security Analyst, InGuardians
- Jeffrey E. Dagle, Chief Electrical Engineer, Energy Technology Development, Pacific Northwest National Laboratory
- David Dunn, Manager, Organizational Governance Support, Independent Electricity System Operator
- Robert Former, Principal Security Engineer, Itron, Inc.
- Travis Goodspeed, Security Consultant, Radiant Machines
- Ed Gray, Vice President, Legislative and Regulatory Affairs, Elster Solutions
- Donny Helm, Manager of Technology, Electric Delivery, Oncor
- Michael Hyland, Vice President of Engineering Services, American Public Power Association
- Stan M. Kaplan, Energy and Environmental Policy Specialist, Congressional Research Service
- Jeffrey S. Katz, Chief Technology Officer, Energy and Utilities Industry, IBM

- Christopher Knudsen, Director, Technology Innovation Center, Pacific Gas & Electric
- Stephen J. Lukasik, Former Director, Defense Advanced Research Projects Agency and Former Chief Scientist, Federal Communications Commission
- Richard Pethia, Director of the CERT program, Carnegie Mellon University Software Engineering Institute
- William H. Sanders, Donald Biggar Willett Professor of Engineering, Director, Information Trust Institute, and Acting Director, Coordinated Science Laboratory, University of Illinois
- Christopher Villarreal, Regulatory Analyst, California Public Utilities Commission
- David Wollman, Manager, Electrical Metrology Groups, National Institute of Standards and Technology
- Andrew Wright, Chief Technology Officer, N-Dimension Solutions
- Christine Wright, Team Leader, Competitive Markets Division, Public Utility Commission of Texas

# Appendix IV: Comments from the Department of Commerce



**UNITED STATES DEPARTMENT OF COMMERCE**  
**The Secretary of Commerce**  
Washington, D.C. 20230

December 20, 2010

Mr. Gregory C. Wilshusen  
Director, Information Security Issues  
United States Government Accountability Office  
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to comment on the draft report entitled "Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed" (GAO-11-117).

We agree with the report's recommendations that (1) the National Institute of Standards and Technology (NIST) finalize its plan and schedule for updating its cybersecurity guidelines, and (2) the Federal Energy Regulatory Commission develop a coordinated approach to monitor voluntary standards and address any gaps in compliance. We offer the following comments regarding GAO's conclusions.

1. Throughout the report, replace "missing key elements" with "NIST's follow-on cyber-physical activity."
2. Page 16. Delete the following two sentences in the first paragraph: "As a part of this assessment, NIST planned to address other key elements of cybersecurity, including the impact of coordinated cyber-physical attacks, and identifying smart grid system vulnerabilities. The working group intended to complete these efforts and issue the guidelines in June 2010." NIST stated that it plans to include these elements in revisions to the guidelines that were issued in September 2010, not those issued in June 2010. These sentences incorrectly imply that NIST has not completed planned activities related to cyber-physical attacks.
3. Page 29. NIST agrees that the risk of combined cyber-physical attacks on the smart grid is an area that needs to be more fully explored in the future, but disagrees with the statement that NIST was planning to cover it in the August 2010 final document. That document states that follow-on activities of the Cybersecurity Working Group need to address cyber-physical attacks.

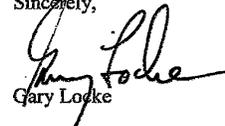
Therefore, we suggest changing the wording of the recommendation to "To ensure that NIST's smart grid cybersecurity guidelines will be as effective as intended, we

Mr. Gregory C. Wilshusen  
Page 2

recommend that the Director of NIST finalize the agency's plan for updating and maintaining the cybersecurity guidelines, including ensuring it incorporates (1) an assessment of the types and effects of combined cyber-physical attacks and (2) specific milestones for when efforts are to be completed. We also recommend that NIST, as a part of finalizing the plan, assess whether any cybersecurity challenges identified in this report should be addressed in the guidelines."

Please contact Rachel Kinney, NIST Management and Program Analyst, at (301) 975-8707; if you have any questions regarding this response. We look forward to receiving your final report.

Sincerely,



Gary Locke

# Appendix V: Comments from the Federal Energy Regulatory Commission

FEDERAL ENERGY REGULATORY COMMISSION  
WASHINGTON, DC 20426

OFFICE OF THE CHAIRMAN

December 23, 2010

Mr. David A. Powner  
Director, Information Technology Management Issues  
United States Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Mr. Powner:

Thank you for your December 1, 2010 electronic transmission of the draft report, *Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed*. I appreciate the opportunity to comment on this draft report.

The draft report identifies a number of challenges to securing smart grid systems and evaluates, among other things, the Federal Energy Regulatory Commission's (Commission) approach for adopting and monitoring cybersecurity and other standards for the smart grid. In general, I commend the draft report's useful discussion of cybersecurity for the electric industry, and I appreciate its helpful conclusions. I respond to the report's specific recommendations in more detail below and also present two more general issues.

In order to improve coordination among regulators and help Congress better assess the effectiveness of the process established in the Energy Independence and Security Act of 2007 (EISA) for developing voluntary smart grid standards, the draft report recommends that the Commission coordinate with state regulators and groups that represent utilities subject to limited Commission and state regulation (such as municipal and cooperative utilities) to: (1) periodically evaluate the extent to which utilities and manufacturers are following voluntary interoperability and cybersecurity standards adopted through the EISA process, and (2) develop strategies for addressing any gaps in compliance that are identified as a result of this evaluation. To the extent that the Commission determines that, despite this coordinated approach, it lacks authority to address any gaps in compliance, the draft report recommends reporting this information to Congress.

2

I agree with the recommendation to improve coordination among regulators. I will direct the Commission's staff to evaluate possible approaches for implementing this recommendation. I note that the Smart Response Collaborative of the Commission and the National Association of Regulatory Utility Commissioners recently held a technical conference on smart grid standards. I also note that the Commission must operate within its statutory authority, which may limit the tools at the Commission's disposal. Therefore, if the Commission finds that it lacks authority to address gaps in compliance with voluntary interoperability and cybersecurity standards adopted through the EISA process, I will report this information to Congress, as the draft report recommends.

The draft report also recommends that the Commission, working in conjunction with the North American Electric Reliability Corporation as appropriate, assess whether any of the challenges identified in the draft report should be addressed in Commission cybersecurity efforts. I agree with this recommendation, as well, and I have directed Commission staff to develop appropriate procedures to achieve this goal. I again note, however, that the Commission must operate within its statutory authority.

Apart from the foregoing, I would like to present two more general issues. First, the last challenge identified in the draft report is that the lack of electricity industry cybersecurity metrics makes it difficult to measure the extent to which investments in cybersecurity improve the security of smart grid systems. The draft report also recognizes experts' observation that such metrics are difficult to develop. I agree with the importance of such metrics, and would emphasize the need for the metrics to be specific and fine-tuned enough to differentiate validly among investments based on the strength of their cybersecurity protections.

Second, the draft report appears to assume that Congress intended for all relevant manufacturers and utilities to comply with the smart grid standards adopted through the EISA process. It could reasonably be argued, however, that in making these smart grid standards voluntary, Congress was not seeking to ensure this outcome. If the report is assuming a Congressional intent of uniform compliance with the standards adopted through the EISA process, it may be helpful to state more clearly both that position and the basis upon which it was reached.

---

**Appendix V: Comments from the Federal  
Energy Regulatory Commission**

---

3

Thank you again for the opportunity to comment on your report. Your recommendations generally represent meaningful measures to improve coordination among regulators, help Congress better assess the effectiveness of the process established in EISA for developing voluntary smart grid standards and expand the Commission cybersecurity efforts, as needed.

Sincerely,



Jon Wellinoff  
Chairman

---

# Appendix VI: GAO Contacts and Staff Acknowledgments

---

## GAO Contact

David A. Powner (202) 512-9286 or [pownerd@gao.gov](mailto:pownerd@gao.gov)

David C. Trimble (202) 512-3841 or [trimbled@gao.gov](mailto:trimbled@gao.gov)

---

## Staff Acknowledgments

In addition to the individuals named above, key contributions were made to this report by Gary N. Mountjoy, Assistant Director, IT; Jon R. Ludwigson, Assistant Director, NRE; Nabajyoti Barkakati; Scott F. Borre; Camille M. Chaires; Neil J. Doherty; Rebecca E. Eyler; Paige M. Gilbreath; Lee A. McCracken; Thomas E. Murphy; Andrew S. Stavisky; Walter K. Vance; and Maria P. Vargas.

---

# Related GAO Products

---

## Critical Infrastructure

*Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience.* [GAO-10-296](#). Washington, D.C.: March 5, 2010.

*Defense Critical Infrastructure: Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DOD Critical Assets.* [GAO-10-147](#). Washington, D.C.: October 23, 2009.

*Critical Infrastructure Protection: OMB Leadership Needed to Strengthen Agency Planning Efforts to Protect Federal Cyber Assets.* [GAO-10-148](#). Washington, D.C.: October 15, 2009.

*Critical Infrastructure Protection: Current Cyber Sector-Specific Planning Approach Needs Reassessment.* [GAO-09-969](#). Washington, D.C.: September 24, 2009.

*Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies.* [GAO-08-64T](#). Washington, D.C.: October 31, 2007.

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

*Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve.* [GAO-07-706R](#). Washington, D.C.: July 10, 2007.

*Critical Infrastructure: Challenges Remain in Protecting Key Sectors.* [GAO-07-626T](#). Washington, D.C.: March 20, 2007.

*Critical Infrastructure Protection: Challenges in Addressing Cybersecurity.* [GAO-05-827T](#). Washington, D.C.: July 19, 2005.

---

## Cybersecurity

*Cybersecurity: Continued Efforts Are Needed to Protect Information Systems from Evolving Threats.* [GAO-10-230T](#). Washington, D.C.: November 17, 2009.

*Cybersecurity: Continued Federal Efforts Are Needed to Protect Critical Systems and Information.* [GAO-09-835T](#). Washington, D.C.: June 25, 2009.

---

## Electricity and Energy Markets

*Transmission Lines: Issues Associated with High-Voltage Direct-Current Transmission Lines along Transportation Rights of Way.* [GAO-08-347R](#). Washington, D.C.: February 1, 2008.

*Meeting Energy Demand in the 21st Century: Many Challenges and Key Questions.* [GAO-05-414T](#). Washington, D.C.: March 16, 2005.

*Electricity Markets: Consumers Could Benefit from Demand Programs, but Challenges Remain.* [GAO-04-844](#). Washington, D.C.: August 13, 2004.

*Energy Markets: Additional Actions Would Help Ensure That FERC's Oversight and Enforcement Capability Is Comprehensive and Systematic.* [GAO-03-845](#). Washington, D.C.: August 15, 2003.

*Electricity Markets: FERC's Role in Protecting Consumers.* [GAO-03-726R](#). Washington, D.C.: June 6, 2003.

---

## Electricity Restructuring

*Electricity Restructuring: FERC Could Take Additional Steps to Analyze Regional Transmission Organizations' Benefits and Performance.* [GAO-08-987](#). Washington, D.C.: September 22, 2008.

*Electricity Restructuring: Key Challenges Remain.* [GAO-06-237](#). Washington, D.C.: November 15, 2005.

*Electricity Restructuring: 2003 Blackout Identifies Crisis and Opportunity for the Electricity Sector.* [GAO-04-204](#). Washington, D.C.: November 18, 2003.

*Electricity Restructuring: Action Needed to Address Emerging Gaps in Federal Information Collection.* [GAO-03-586](#). Washington, D.C.: June 30, 2003.

*Lessons Learned from Electricity Restructuring: Transition to Competitive Markets Under Way, but Full Benefits Will Take Time and Effort to Achieve.* [GAO-03-271](#). Washington, D.C.: December 17, 2002.

*Restructured Electricity Markets: California Market Design Enabled Exercise of Market Power.* [GAO-02-828](#). Washington, D.C.: June 21, 2002.

*Restructured Electricity Markets: Three States' Experiences in Adding Generating Capacity.* [GAO-02-427](#). Washington, D.C.: May 24, 2002.

---

Information Security

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

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site ([www.gao.gov](http://www.gao.gov)). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to [www.gao.gov](http://www.gao.gov) and select "E-mail Updates."

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Ralph Dawn, Managing Director, [dawnr@gao.gov](mailto:dawnr@gao.gov), (202) 512-4400  
U.S. Government Accountability Office, 441 G Street NW, Room 7125  
Washington, DC 20548

---

## Public Affairs

Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548

