U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE AND TECHNOLOGY
SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

HEARING CHARTER

Smart Grid Architecture and Standards: Assessing Coordination and Progress

Thursday, July 1, 2010
10:00 a.m.—12:00 p.m.
2318 Rayburn House Office Building

Witnesses

- **Dr. George Arnold:** National Coordinator for Smart Grid**,** National Institute of Standards and Technology
- **Mr. Mason Emnett:** Associate Director of the Office of Energy Policy and Innovation, Federal Energy Regulatory Commission
- **Mr. John McDonald:** Director of Technical Strategy and Policy Development, GE Energy
- **Mr. Conrad Eustis:** Director of Retail Technology Development, Portland General Electric
- **Ms. Lillie Coney:** Associate Director, Electronic Privacy Information Center

Purpose

As directed by the Energy Independence and Security Act (EISA) of 2007 (P.L. 110-140), the National Institute of Standards and Technology (NIST) is coordinating an effort to develop a common framework and interoperability standards for the smart grid. The purpose of this hearing is to examine the progress of this effort and discuss how standards affect the development of the smart grid and the deployment of smart grid technologies. Additionally, witnesses will discuss current and anticipated challenges associated with these standards and offer their views on the ability of the current process to meet these challenges and develop standards that will enable the growth of a reliable, efficient, and secure smart grid.

Overview

The term "smart grid" refers to modernization of the electric grid to incorporate digital computing, microprocessor-based measurement and control, and communication technology. These technologies will enable greater two-way communication between consumers and electricity providers so that consumers can adjust their electricity usage in response to real-time

demand and price information. These technologies will also enable two-way energy transfer, or the ability for consumers to feed surplus energy into the grid, and will help accommodate widespread use of different types of electricity generation and storage options, from solar roofing shingles to electric vehicles. Other anticipated benefits of the smart grid include: better regulation of power quality (i.e., minimizing the fluctuations in voltage which can damage more sensitive electronics and other equipment); more efficient use of power generating infrastructure; greater resiliency of the electric grid infrastructure in withstanding disasters; and economic growth from the new products and services created for, and by, the smart grid.

The smart grid is often referred to as a system of systems and a network of networks. Given its highly interconnected nature, standards are essential to ensuring that smart grid components will work together effectively and efficiently. Section 1305 of EISA directed NIST to work with Federal, State, and private-sector stakeholders to develop a smart grid interoperability framework that is "flexible, uniform, and technology neutral." An interoperability framework creates a model of a complex system, like the smart grid. It helps identify where information exchange needs to take place between devices and networks to meet the functional requirements of the system.

With $15 million in Recovery Act funding, NIST has brought together over 1,500 interested parties, from power generators and utility regulators, to high-tech companies and software developers, to develop a conceptual architecture, or framework, for the smart grid and to coordinate the development of standards. Through this effort, NIST has already identified 75 existing standards, in varying stages of development that have smart grid applications. NIST also performed a gap analysis to identify areas lacking necessary standards. This analysis revealed 70 gaps.

NIST created 16 Priority Action Plans (PAPs) to engage the appropriate experts and develop, or refine, the most urgently needed standards on a fast-track timeline. The initial efforts will address needs in eight priority areas, including energy storage and Advanced Metering Infrastructure. Such standards are critical to creating viable consumer technology and for enabling the envisioned environmental benefits, such as distributed power generation and widespread adoption of plug-in electric vehicles.

In conjunction with the development of interoperability standards, NIST is coordinating the development of cyber security standards to ensure the security and privacy of smart grid data and systems.

According to NIST, the initial 75 standards represent only a "small subset of the totality of standards that will ultimately be required to build a safer, secure smart grid that is interoperable, end to end." Therefore, the agency has formed the Smart Grid Interoperability Panel (SGIP) to continue to oversee this standards coordination process. Nearly 600 stakeholder organizations are part of the SGIP, which will help identify additional priority areas for standards development and serve as a forum to resolve any issues that emerge during the standards development process. NIST is also working to develop a testing and evaluation framework for smart grid technology to ensure that products that are sold perform as intended.

EISA requires that the Federal Energy Regulatory Commission (FERC) adopt into rulemaking "standards and protocols that ensure smart grid functionality and interoperability in interstate transmission of electric power, and regional, and wholesale electricity markets." From the initial 75 existing standards with applicability to the smart grid, FERC is preparing to initiate rulemaking on 14 of these standards.

Background

Overview of Smart Grid

The smart grid encompasses a wide array of technology that has the potential to dramatically improve the reliability, security, and efficiency of the electric grid, offering economic and environmental benefits. As described in more detail below, the existing grid is a patchwork of systems that pose reliability and security concerns, and limit opportunities for energy efficiency and conservation.

Reliability. Congestion on the electric grid is a growing problem. At its worst, congestion can damage transmission lines and lead to major blackouts, like the one in 2003 that darkened large portions of the Northeast and the Midwest. Since electricity cannot be stored and must be used as soon as it is generated, the operators of the transmission system must carefully coordinate the routing of power from a number of sources through a limited number of pathways. Over the past several decades, growing electricity demand has pushed the limits of the transmission infrastructure, creating bottlenecks at major high-voltage lines around the country, especially during peak demand periods. Exceeding the capacity of these pathways can cause brownouts, or worse, power outages and damage to infrastructure as lines and equipment become overheated. Failure at these junctions can disrupt the balance between electricity generation and usage, spreading disruption to other parts of the grid. According to the Department of Energy, outages affected 15 percent more customers from 1996 to 2000 than from 1991 to 1995[1].

Modern smart grid technologies can improve reliability. With the existing grid, the slow response time of mechanical switches, a lack of automated analysis capabilities, and operators' low situational awareness—or detailed visibility—of the grid make the task of routing power more challenging and more prone to failure. Smart grid technologies will seek to provide "wide area situational awareness," which will integrate real-time sensor data, weather information, and grid modeling with geographic information systems. This will enable grid operators to instantly switch between views that show the status of the grid for an entire region to views that show current conditions of the grid in individual neighborhoods. In addition, smart grid technologies are intended to allow operators to improve diagnosis of grid disturbances, precisely locating problems and optimizing repairs.

Efficiency and Conservation. In addition to increasing the reliability of electricity transmission and distribution, smart grid technologies can enable greater energy efficiency and conservation and reduce emissions. The Department of Energy estimates that if the grid were just 5 percent more efficient, the emissions and fuel savings would be the equivalent of removing 53 million cars from the road[2].

[1] *The Smart Grid: An Introduction*. The Department of Energy, 2008. Pg. 7.
[2] *The Smart Grid: An Introduction*. The Department of Energy, 2008. Pg. 7.

As noted above, congestion in the transmission lines has a major impact on grid operation. The most efficient power plants are larger "baseload plants" which operate continuously and generally meet the average customer demand in their service areas. Although demand during peak periods does not often exceed the generating capacity of these plants, it can exceed the capacity of the transmission lines. At such times, operators must bring additional, less efficient "peaking plants" online, which are often closer to the service area. One of the major anticipated benefits of the smart grid is technologies to help reduce demand during peak periods, reducing the need to draw on less efficient plants. A major component of the smart grid will be advanced metering infrastructure that provides real-time information directly to consumers, enabling them to see their own usage and react to higher demand—and higher prices—by using less electricity. These technologies, coupled with smart appliances, could also be used by utilities to quickly stem demand when it exceeds transmission capacity.

In addition to demand-response pricing, the smart grid will also enable increased use of renewable sources of energy and the use of distributed energy storage devices. Advanced communication and computational technologies will allow the grid to remain in balance while drawing on intermittent renewable energy sources, such as wind and solar. It will also enable the integration of solar roofing shingles and other small-scale distributed renewable sources. The technology exists to connect renewable resources like these to the grid. However, they are far short of the "plug and play" capabilities needed to promote widespread adoption. They also do not incorporate technologies which would allow them to interact dynamically with the grid. Smart grid technologies hold the possibility of using electric vehicle batteries as energy storage devices that could feed energy back onto the grid. Plug-in electric vehicles and plug-in hybrid electric vehicles could help balance the large swings in demand over the course of a day by charging at night when demand is lowest, and returning power to the grid during the day when demand reaches its height (often termed peak-shaving). Through demand-response pricing, which will be enabled by smart grid, consumers will have an incentive to charge their vehicles at night.

Security. The centralized control systems that manage and control the generation, transmission, and distribution of electric power raise significant cyber security concerns. These control systems monitor and control sensitive processes and physical functions on the grid, including opening and closing circuit breakers and setting thresholds for preventative shutdowns. In 2007, the Government Accountability Office (GAO) released a report highlighting the vulnerability of these control systems to cyber security attacks or unintentionally caused system disturbances[3]. The report cited a number of factors, including the interconnectivity of these systems, their connection to the Internet, non-secure connections, and the availability of pertinent technical information, that make supervisory control and data acquisition systems susceptible to cyber threats and vulnerabilities. There are dozens of examples from around the world of malicious exploitation of vulnerabilities in control systems, or simple control system malfunctions, that caused serious consequences in the functioning of critical infrastructure.

[3] *Critical infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain.* The Government Accountability Office, 2007. Pgs. 3-18.

With their increased reliance on networked communication systems, smart grid technologies have the potential to pose additional cyber security risks. Not only is there fear that non-secure systems could open the door to widespread power disruption, there is also fear that the storage and communication of real-time energy usage data could be a risk to consumer privacy.

Standards

A common smart grid framework—or architecture—and technical standards are recognized as essential to realizing the potential benefits of the smart grid. This requires collaboration between industry sectors that have never before had to work together toward a common goal. Figure 1, which is the Conceptual Reference Model for Smart Grid Information Networks developed by NIST and associated stakeholders, illustrates this complex web of actors, grouped into domains where similar functions take place (e.g., the home, transmission systems, or power plants). Dozens of devices and systems must communicate under the proposed smart grid architecture, requiring common data sharing protocols and common methods of presenting information. In addition, the architecture should be flexible to allow the incorporation of evolving technologies, while still supporting legacy systems and devices.

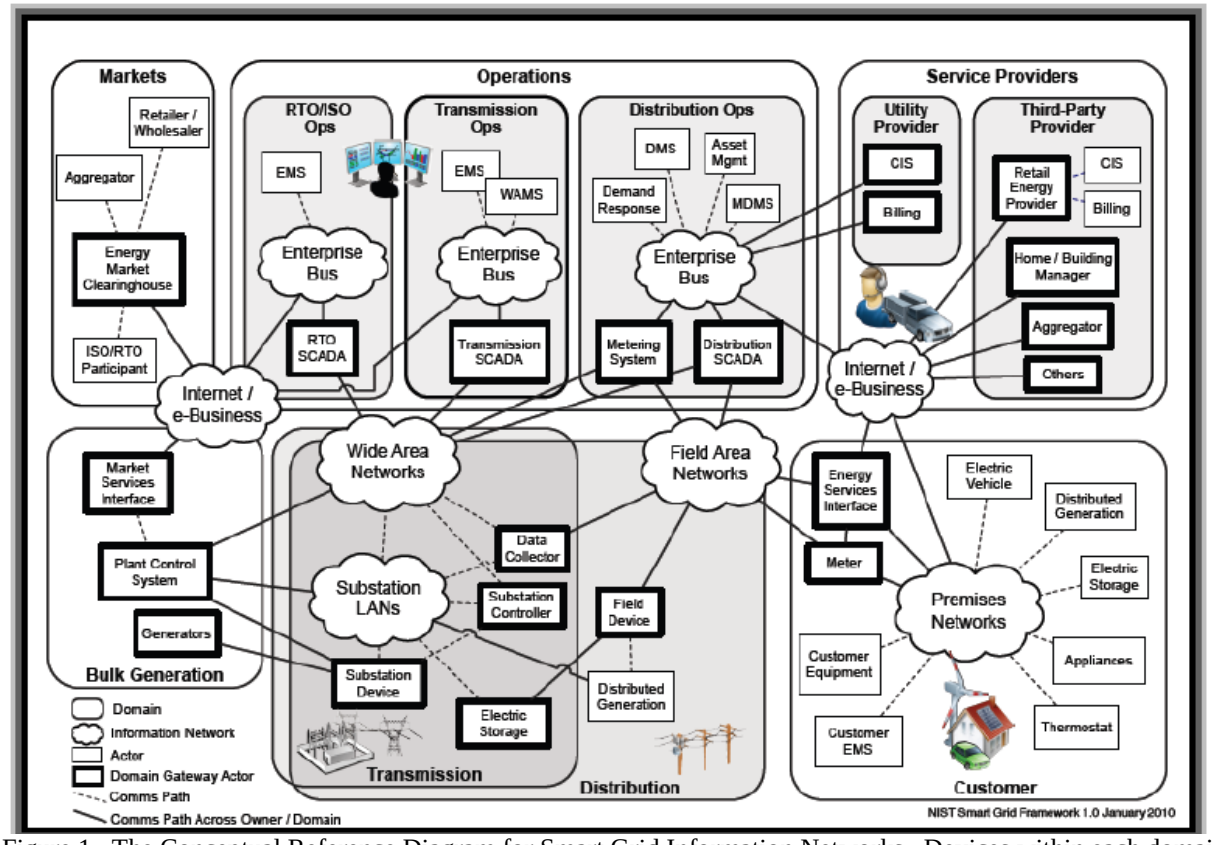

Figure 1. The Conceptual Reference Diagram for Smart Grid Information Networks. Devices within each domain (customer; markets; service providers; operations; bulk generation; transmission; and distribution) must communicate across a number of interfaces.

The NIST-led framework development and standards identification process described in the Overview section culminated in the January 2010 release of the *NIST Framework and Roadmap*

for Smart Grid Interoperability Standards, Release 1.0. As discussed in the Overview section above, this document identified a number of smart grid-related standards and standards gaps. From these, NIST created 16 Priority Action Plans (PAPs) to address standards needs that will be fundamental to achieving smart grid benefits, such as greater consumer visibility and control of electricity usage and greater use of distributed renewable energy sources.

Three of the PAPs included in the NIST Framework are devoted to smart grid communications. The standards addressed by these PAPs—Guidelines for the Use of IP Protocol Suite in the Smart Grid, Guidelines for Use of Wireless Communication, and Harmonization of Power Line Carrier Standards for Appliance Communications in the Home—will ensure that smart appliances and other home systems can communicate with home area networks and advanced smart meters without requiring technological expertise and configuration by consumers, and without interfering with one another. For example, currently, manufacturers are considering several power line-based communication technologies for appliances, meters, and plug-in electric vehicle communications. A number of technologies currently exist, but they are not interoperable and some may actually interfere with one another. Thus these standards are critical to widespread adoption of smart grid technologies because consumers are unlikely to choose smart appliances unless they are smart, interoperable, and compatible.

As discussed above, the smart grid holds the potential for electric vehicles to act as demand-stabilizing power storage devices and also for the penetration of renewables onto the grid. In response, work is currently underway on two PAPs, Energy Storage Interconnection Guidelines and Interoperability Standards to Support Plug-in Electric Vehicles. The objective of this work is to develop standards and guidelines for connecting these power sources and storage devices to the grid in a way that addresses potential intermittency and variability and is responsive to grid management requirements.

The cyber security vulnerabilities of the electric grid are not new, but smart grid technologies will likely pose a more complex cyber security challenge. For example, with advanced metering infrastructure, third-party service providers (e.g., a web-based customer energy usage interface), smart appliances, and other smart grid features, there will be a greater number of entry points through which to stage cyber attacks. Moreover, the increased complexity of the grid could introduce vulnerabilities and increase exposure to potential attackers or unintentional disruptions.

In addition to the more traditional risks of reliability, smart grid technologies may also create vulnerabilities around customer privacy. Real-time energy usage data can reveal personal habits, for example, revealing how many occupants live in a home and when they generally leave and return to the home. This information could even reveal detailed aspects of daily and weekly routines, such as when occupants of a home shower, and how often they run the washing machine.

NIST has made cyber security a priority, initiating a separate cyber security process to complement the overall smart grid standards development process. Through a 300 member Smart Grid Cyber Security Coordination Task Group, NIST is coordinating "the development of measures to ensure the confidentiality, integrity and availability of the electronic information communication systems and the control systems necessary for the management, operation, and

protection of the grid." This task group released a draft version of the *Cyber Security Guidelines* early this year. In this document, the developers identify the risks associated with smart grid and the relevant security requirements for the smart grid. The work generated from this effort is intended to enable cyber security to be an integral part of the design process as the smart grid architecture and standards evolve.

Regulation

In the U.S., the power industry is highly fragmented, with over 3,100 entities under various forms of private investor and public ownership. By authority of the Federal Power Act, FERC has jurisdiction to regulate the wholesale power market and electric system reliability standards. However, a patchwork of state regulations govern electric industry structure, generation adequacy, energy resource mix, transmission siting, cost recovery, and retail electricity prices.

Power-related regulations have evolved over time as utilities became increasingly interconnected. By the mid-part of the 20th century, through ad-hoc growth, the power system in the U.S. had become highly interconnected. A major power outage in 1965, which quickly cascaded to cover the entire Northeast, illustrated the lack of high-level planning to prevent and prepare for outages. It also revealed that operators within the large interconnected zone did not have common operating standards and procedures. Created by legislation in response to the 1965 blackout, the North American Electric Reliability Council began to develop regional standards of operation to ensure reliability of the grid. After the major 2003 blackout which also blanketed the Northeast, these standards were adopted into regulation by FERC.

The *NIST Framework* notes that the transition to the smart grid introduces new regulatory considerations, including security, reliability, safety, privacy, and other policy considerations, which "may transcend jurisdictional boundaries and require increased coordination among federal, state, and local lawmakers and regulators." To that end, the common architecture developed through the NIST process is intended to help facilitate and enable this coordination.

Issues and Concerns

Even though the technologies are young, there has already been significant investment in the smart grid. The American Recovery and Reinvestment Act invested $9.2 billion ($4.5 billion in federal funds; $4.7 billion in matching funds from private companies, utilities, cities, and other partners) in smart grid related technologies, including smart meters, software to manage meter and grid data, and distributed energy generation resources. The U.S. market for smart grid related equipment, devices, information and communication technologies, and other hardware, software, and services is expected to reach $47 billion per year by 2014. Globally, this market is projected to reach $171 billion[4]. Given the scale of investment, ensuring interoperability is imperative.

Standards development is typically a time intensive process, reflecting the complexity and requirement for consensus. However, given that modernizing the electric grid has been

[4] *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0,* January 2010, Pg. 14.

identified as a national priority, NIST has called for aggressive timelines for a number of the standards. An important challenge will be maintaining a pace of standards development that will ensure interoperability and encourage additional investment, but also maintain the quality of the standards and ensuring that they are open, flexible, and meet reliability, security, and efficiency needs.

The Cyber Security Coordination Task Group described above performed a Privacy Impact Assessment for the customer interface portion of the smart grid. This assessment found that a lack of consistent and comprehensive privacy policies, standards, and supporting procedures throughout the states, government agencies, utility companies, and supporting entities that will be involved in smart grid data collection and management created privacy risks that would need to be addressed.

As noted above, there is a sizable global market for smart grid technologies, and many countries are also planning to move to smart grid technologies. U.S. manufacturers stand to lead in the market for smart grid technologies, making international engagement an important aspect of the Nation's own smart grid development. NIST has engaged with smart grid stakeholders in other countries and is promoting a common smart grid framework. In addition, of the 75 existing standards listed in the *NIST Framework,* 13 percent came from domestic standards development organizations (SDOs), 10 percent from the U.S. Government, and 77 percent were from international SDOs.

As noted above, NIST intends to incorporate testing and evaluation into the overall smart grid standards process to ensure that technology will perform as intended. Although NIST has designated testing and evaluation as the final phase in meeting the requirements of EISA, it has been included in the work of the SGIP and the development of a framework for testing and evaluation is currently underway. The fact that there is not yet a formal testing and evaluation process for all smart grid technologies raises important questions about the consistent implementation of existing standards.