

# SMART GRID ARCHITECTURE AND STANDARDS: ASSESSING COORDINATION AND PROGRESS

---

---

HEARING  
BEFORE THE  
SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION  
COMMITTEE ON SCIENCE AND  
TECHNOLOGY  
HOUSE OF REPRESENTATIVES  
ONE HUNDRED ELEVENTH CONGRESS  
SECOND SESSION  
JULY 1, 2010  
**Serial No. 111-104**

Printed for the use of the Committee on Science and Technology



Available via the World Wide Web: <http://www.science.house.gov>

---

U.S. GOVERNMENT PRINTING OFFICE

57-602PDF

WASHINGTON : 2010

---

For sale by the Superintendent of Documents, U.S. Government Printing Office  
Internet: [bookstore.gpo.gov](http://bookstore.gpo.gov) Phone: toll free (866) 512-1800; DC area (202) 512-1800  
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON SCIENCE AND TECHNOLOGY

HON. BART GORDON, Tennessee, *Chair*

JERRY F. COSTELLO, Illinois	RALPH M. HALL, Texas
EDDIE BERNICE JOHNSON, Texas	F. JAMES SENSENBRENNER JR., Wisconsin
LYNN C. WOOLSEY, California	LAMAR S. SMITH, Texas
DAVID WU, Oregon	DANA ROHRABACHER, California
BRIAN BAIRD, Washington	ROSCOE G. BARTLETT, Maryland
BRAD MILLER, North Carolina	VERNON J. EHLERS, Michigan
DANIEL LIPINSKI, Illinois	FRANK D. LUCAS, Oklahoma
GABRIELLE GIFFORDS, Arizona	JUDY BIGGERT, Illinois
DONNA F. EDWARDS, Maryland	W. TODD AKIN, Missouri
MARCIA L. FUDGE, Ohio	RANDY NEUGEBAUER, Texas
BEN R. LUJÁN, New Mexico	BOB INGLIS, South Carolina
PAUL D. TONKO, New York	MICHAEL T. McCAUL, Texas
STEVEN R. ROTHMAN, New Jersey	MARIO DIAZ-BALART, Florida
JIM MATHESON, Utah	BRIAN P. BILBRAY, California
LINCOLN DAVIS, Tennessee	ADRIAN SMITH, Nebraska
BEN CHANDLER, Kentucky	PAUL C. BROUN, Georgia
RUSS CARNAHAN, Missouri	PETE OLSON, Texas
BARON P. HILL, Indiana	
HARRY E. MITCHELL, Arizona	
CHARLES A. WILSON, Ohio	
KATHLEEN DAHLKEMPER, Pennsylvania	
ALAN GRAYSON, Florida	
SUZANNE M. KOSMAS, Florida	
GARY C. PETERS, Michigan	
JOHN GARAMENDI, California	
VACANCY	

---

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

HON. DAVID WU, Oregon, *Chair*

DONNA F. EDWARDS, Maryland	ADRIAN SMITH, Nebraska
BEN R. LUJÁN, New Mexico	JUDY BIGGERT, Illinois
PAUL D. TONKO, New York	W. TODD AKIN, Missouri
HARRY E. MITCHELL, Arizona	PAUL C. BROUN, Georgia
GARY C. PETERS, Michigan	
JOHN GARAMENDI, California	
BART GORDON, Tennessee	RALPH M. HALL, Texas

MIKE QUEAR *Subcommittee Staff Director*

MEGHAN HOUSEWRIGHT *Democratic Professional Staff Member*

TRAVIS HITE *Democratic Professional Staff Member*

HOLLY LOGUE *Democratic Professional Staff Member*

MELE WILLIAMS *Republican Professional Staff Member*

VICTORIA JOHNSTON *Research Assistant*

# CONTENTS

July 1, 2010

Witness List .....	Page 2
Hearing Charter .....	3

## Opening Statements

Statement by Representative David Wu, Chairman, Subcommittee on Technology and Innovation, Committee on Science and Technology, U.S. House of Representatives .....	9
Written Statement .....	10
Statement by Representative Adrian Smith, Ranking Minority Member, Subcommittee on Technology and Innovation, Committee on Science and Technology, U.S. House of Representatives .....	11
Written Statement .....	12

## Witnesses:

Dr. George W. Arnold, National Coordinator for Smart Grid, National Institute of Standards and Technology	
Oral Statement .....	13
Written Statement .....	15
Biography .....	21
Mr. Mason W. Emmett, Associate Director of The Office of Energy Policy and Innovation, Federal Energy Regulatory Commission	
Oral Statement .....	22
Written Statement .....	23
Biography .....	26
Mr. John D. McDonald, P.E., Director of Technical Strategy and Policy Development, GE Energy	
Oral Statement .....	27
Written Statement .....	28
Biography .....	37
Mr. Conrad Eustis, Director of Retail Technology Development, Portland General Electric	
Oral Statement .....	38
Written Statement .....	39
Biography .....	43
Ms. Lillie Coney, Associate Director, Electronic Privacy Information Center	
Oral Statement .....	43
Written Statement .....	45
Biography .....	59

## Appendix 1: Answers to Post-Hearing Questions

Dr. George W. Arnold, National Coordinator for Smart Grid, National Institute of Standards and Technology .....	86
Mr. John D. McDonald, P.E., Director of Technical Strategy and Policy Development, GE Energy .....	87
Mr. Conrad Eustis, Director of Retail Technology Development, Portland General Electric .....	88

IV

**Appendix 2: Additional Material for the Record**

Page

Verbal Questions from Subcommittee by Chairman David Wu .....	90
---	----

**SMART GRID ARCHITECTURE AND STAND-  
ARDS: ASSESSING COORDINATION AND  
PROGRESS**

---

**THURSDAY, JULY 1, 2010**

HOUSE OF REPRESENTATIVES,  
SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION,  
COMMITTEE ON SCIENCE AND TECHNOLOGY,  
*Washington, DC.*

The Subcommittee met, pursuant to call, at 10:04 a.m., in Room 2318 of the Rayburn House Office Building, Hon. David Wu [Chairman of the Subcommittee] presiding.

**Subcommittee on Technology and Innovation's**

Hearing on

**Smart Grid Architecture and Standards: Assessing  
Coordination and Progress**

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

**Witness List**

**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

## HEARING CHARTER

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

**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 Emmett:** 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.<sup>1</sup>

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.

<sup>1</sup>*The Smart Grid: An Introduction*. The Department of Energy, 2008. p. 7.

**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 five percent more efficient, the emissions and fuel savings would be the equivalent of removing 53 million cars from the road.<sup>2</sup>

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.<sup>3</sup> 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.

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

<sup>2</sup>*The Smart Grid: An Introduction.* The Department of Energy, 2008. p. 7.

<sup>3</sup>*Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain.* The Government Accountability Office, 2007. pp. 3–18.

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.

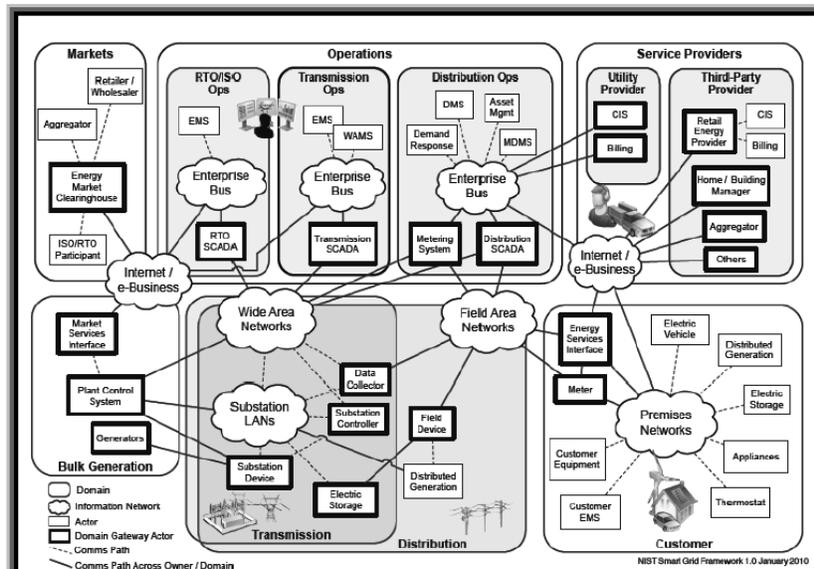


Figure 1. The Conceptual Reference Diagram for Smart Grid Information Networks. Devices within each domain (customer; markets; service providers; operations; bulk generation; transmission; and distribution) must communicate across a number of interfaces.

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.<sup>4</sup> 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 identified as a national priority, NIST has called for aggressive

<sup>4</sup>*NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, January 2010, p. 14.

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), 111 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.

Chairman WU. Good morning. Welcome to everyone. Thank you for coming to this first in a—well, one in a series of hearings on smart grid and smart grid-related issues. The enterprise that we are embarking upon, the modernization of our century-old electric power system, is a very, very important step in moving toward a clean and independent energy future. It is critical to developing a more reliable and secure, and as private as possible, electrical grid. My understanding is that about 40 percent of our national energy budget is allocated to electricity, and unfortunately, two-thirds of the total electrical energy that we generate does not arrive in useful form for the end user. So building out a smart grid will enable more efficient use, will enable the use of the addition of renewable sources and allow for better management of electrical transmission and distribution, and hopefully a more reliable network also. It will help support the increasing demand for electricity and our growing reliance on electrically based technologies.

The grid, the smart grid, will incorporate two-way communication for a flow of information throughout a vast interconnected power transmission system. In fact, I think we are going to hear testimony that—actually this is not submitted testimony. This is, I think, in a letter to the Committee that the requirements of this information system may be 100 times what we currently invest in the Internet. In the smart grid future, customers will have access to real-time data on their energy use and on the market price of electricity, and as the demand for electricity increases, consumers will be able to make more-informed choices on how high to set the thermostat and when to run the dishwasher or other appliances, and consumers will also benefit when grid operators have more detailed information on the status of the grid and respond to disruptions more quickly to keep the lights on or prevent brownouts.

The Nation's electrical grid has often been called the biggest machine on earth. With the addition of smart appliances, solar roofing and networks of communication systems, the grid will become even bigger and more complex. The scale and complexity makes it imperative that all of those involved in developing and using the smart grid share a common technical view, or framework, of the system. It is also crucial that the technologies be based on open standards that facilitate interoperability, security, and competition in the marketplace and also that it be technology-neutral.

In addition, I believe that it is very, very important that the standards we set be promulgated internationally so that we do not have the problems that we have had in the past with certain countries trying to develop islands of technology whether it is to gain commercial advantage or otherwise balkanize the international system.

The benefits of a smart grid will come from massive participation and widespread adoption of smart appliances, solar panels, electric vehicles and other technologies that will provide distributed sources and distributed storage. We need the entire system or the distributed system to be plug-and-play. No consumer wants to find out that the smart dishwasher they bought a year ago will not work and that the home network they just purchased will not interoperate with those appliances. Few consumers will install solar panels, wind turbines and fuel cells for their homes if it is

not easy to see how much power they are creating and track the value of their investment.

Utilities also want to avoid stranded costs. The Energy Act of 2007 tasked the National Institute of Standard and Technology, or NIST, with coordinating the standards process. The 1,500 stakeholders or more NIST sought input from to identify an initial set of 75 standards, and the 580 organizations that are represented on the Smart Grid Interoperability Panel, ranging from regional utilities to large technology companies, illustrate the size and complexity of this process. From reports on the process, the National Smart Grid Coordinator, George Arnold, has done an impressive job of marshaling the private- and public-sector expertise and input needed to perform this task and to do so on a very expedited timeline.

Today we will delve into the standards process in more detail, discuss the work that has been done, and see where things are headed. I am particularly interested in the witnesses' views on the strength of this process thus far and when the witnesses think certification systems will be in place to bring more assurances that the technologies will work together as intended. I will also be interested in the progress of addressing privacy and security challenges posed by the smart grid and the level of international engagement that is necessary for the United States to continue its leadership in smart grid technologies and help the rest of the world in achieving a more energy-independent future.

As we are dealing with the horrible aftermath of the BP spill in the Gulf, moving quickly with technology that will break our dependence on oil is imperative. The work that NIST is facilitating right now is an important component of achieving that goal, and I hope we will learn today how we can continue to address this challenge moving forward.

Chairman WU. With that, I would like to recognize the Ranking Member of this Subcommittee, Mr. Smith, for his opening statement.

[The prepared statement of Chairman Wu follows:]

PREPARED STATEMENT OF CHAIRMAN DAVID WU

Good morning, and thanks to all of you for attending today's hearing on smart grid standards.

The modernization of our 100-year-old electric power system is an integral step in moving toward a clean, independent energy future, and it is critical to developing a more reliable and more secure electrical grid. Building out a smart grid will enable the addition of more renewable sources and allow for better management of the electricity transmission and distribution network. In addition, it will help support the increasing demand for electricity and growing reliance on technology.

The smart grid will incorporate two-way communication for a constant flow of information throughout the vast interconnected power transmission system. In the smart grid future, customers will have access to real-time data on their energy usage and the market price of electricity. As the demand for electricity increases, driving the price up, consumers will be able to make more informed choices on how high to set the thermostat and when to run the dishwasher. Consumers will also benefit when grid operators have more detailed information on the status of the grid and can respond to disruptions more quickly to keep the lights on.

The nation's electrical grid has often been called the biggest machine on earth. With the addition of smart appliances, solar roofing shingles, and networks of communication systems, the grid will become bigger and more complex. The scale and complexity makes it imperative that all of those involved in developing and using the smart grid share a common technical view—or framework—of the system. It is

also crucial that the technologies be based on open standards that facilitate interoperability, security, and competition in the marketplace. The benefits of a smart grid will come from massive participation and widespread adoption of smart appliances, solar panels, and electric vehicles, among other technologies, and for that, we need it to be “plug-and-play.” No consumer wants to find out that the smart dishwasher they bought a year ago will not work with the home network they just purchased. And few consumers will install solar panels, wind turbines, or fuel cells for their homes if it’s not easy to see how much power they’re creating and track the value of their investment.

The Energy Act of 2007 tasked the National Institute of Standards and Technology with coordinating the standards process. The 1,500 stakeholders NIST sought input from to identify an initial set of seven standards, and the 580 organizations that are represented on the Smart Grid Interoperability Panel—ranging from regional utilities to large tech companies—illustrate the size and scope of this process. And, from reports on the process, the National Smart Grid Coordinator, George Arnold, has done an impressive job marshalling the private- and public-sector expertise and input needed to perform this task, and to do so on an expedited timeline.

Today we will delve into the standards process in a little more detail, discuss the work that has been done, and see where things are headed. I am particularly interested in the witnesses’ views on the strength of this process thus far and when the witnesses think certification systems will be in place to bring more assurances that the technologies will work together as intended. I will also be interested in the progress of addressing privacy and security challenges posed by the smart grid and the level of international engagement that is necessary for the U.S. to continue its leadership in smart grid technologies.

As we are dealing with the horrible aftermath of the BP spill in the Gulf, moving quickly with technology that will break our dependence on oil is imperative. The work that NIST is facilitating right now is an important component of achieving that goal, and I hope we will learn today how we can continue to address this challenge moving forward.

Mr. SMITH. Thank you, Chairman Wu, for calling today’s hearing to assess coordination and progress in the development of smart grid architecture and standards.

The Energy Independence and Security Act of 2007 directed NIST to coordinate efforts to develop a common framework and interoperability standards for the implementation of smart grid technologies. This direction was both appropriate and necessary. Our electrical grid is an interconnected, cross-border system, and NIST has proven expertise in developing such standards. In my home State of Nebraska, proper implementation of smart grid technologies would not only allow connected consumers to better manage their consumption of energy but could also encourage investment in small-scale technologies to take advantage of available renewable energy resources for home use and selling it onto the grid. Nebraska ranks sixth among states in wind energy potential but lags behind in implementation because of difficulties in getting electricity onto the grid. Likewise, our many small streams and irrigation canals are a potential resource for small-scale hydroelectric power.

I hope we can also address outstanding concerns with implementation, as well. One particular issue I am interested to learn more about is the effect of smart grid implementation on consumer privacy and even choice. On its face, using macro and micro consumer data to optimize the generation and distribution of electricity is a logical step we can take to improve the efficiency of our system. However, we should also know at what level of granularity this data will be gathered and used, and who will be using it. We should also ensure this data is used to enable smarter consumer

decision-making, not to force false choices on consumers or to cut off access to electricity.

I also hope to learn what, if anything, is being done to ensure stimulus dollars dedicated to the smart grid aren't being wasted on infrastructure which won't meet the forthcoming standards, since these standards have not yet been completed.

With that, thank you, Mr. Chairman, again, for calling this hearing and to our witnesses for your efforts and your expertise as we look at implementing these standards and for your presence here today. I look forward to a fruitful session, and I yield back the balance.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF REPRESENTATIVE ADRIAN SMITH

Thank you, Chairman Wu, for calling today's hearing to assess coordination and progress in the development of smart grid architecture and standards.

The Energy Independence and Security Act of 2007 directed the National Institute of Standards and Technology to coordinate efforts to develop a common framework and interoperability standards for the implementation of smart grid technologies. This direction was both appropriate and necessary. Our electrical grid is an interconnected, cross border system, and NIST has proven expertise in developing such standards.

In my home state of Nebraska, proper implementation of smart grid technologies would not only allow connected consumers to better manage their consumption of energy, but could also encourage investment in small scale technologies to take advantage of available renewable energy resources for home use and selling it onto the grid. Nebraska ranks sixth among states in wind energy potential but lags behind in implementation because of difficulties in getting electricity onto the grid. Likewise, our many small streams and irrigation canals are a potential resource for small scale hydroelectric power.

I hope we can also address outstanding concerns with implementation, as well. One particular issue I am interested to learn more about is the effect of smart grid implementation on consumer privacy and choice.

On its face, using macro and micro consumer data to optimize the generation and distribution of electricity is a logical step we can take to improve the efficiency of our system. However, we should also know at what level of granularity this data will be gathered and used, and who will be using it. We should also ensure this data is used to enable smarter consumer decision-making, not to force false choices on consumers or to cut off access to electricity.

I also hope to learn what, if anything, is being done to ensure stimulus dollars dedicated to smart grid aren't being wasted on infrastructure which won't meet the forthcoming standards, since these standards have not yet been completed.

With that, thank you again, Mr. Chairman, for calling this hearing, and to our witnesses for your efforts to implement these standards and your presence here today. I look forward to a fruitful session and I yield back the balance of my time.

Chairman WU. Thank you very much, Mr. Smith.

If there are any other Members who wish to submit opening statements, those opening statements will be inserted into the record at this point.

And now it is my pleasure to introduce our witnesses. Dr. George Arnold is the National Coordinator for Smart Grid at the National Institute of Standards and Technology. Welcome. Mr. Mason Emmett is the Associate Director of the Office of Energy Policy and Innovation at the Federal Energy Regulatory Commission. We are going to rename Federal agencies like Dave or Joe. Mr. John McDonald is the Director of Technical Strategy and Policy Development at GE Energy. Mr. Conrad Eustis is the Director of Retail Technology Development at Portland General Electric. And our final witness is Ms. Lillie Coney, who is the Associate Director of the Electronic Privacy Information Center.

With that, you will each have five minutes for your spoken testimony. Your written testimonies will be included in the record in their entirety, and when you complete all of your testimony, we will begin with questions. Each Member will have five minutes to question the panel, and I have already spoken with the witnesses about this, but for the information of everyone in the room, we expect votes fairly soon, and what I would like to do is, as much as possible, get through everyone's testimony before votes, proceed with questioning as far as we can, recess for the votes because there are going to be three votes, and then we will, if necessary, come back after those votes and complete the questions and the rest of the hearing.

Dr. Arnold, please proceed.

**STATEMENT OF DR. GEORGE W. ARNOLD, NATIONAL COORDINATOR FOR SMART GRID, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**

Dr. ARNOLD. Chairman Wu, thank you for the opportunity to—  
Chairman WU. Dr. Arnold, I believe that there is a switch in front of you. It is not a smart microphone, so—

Dr. ARNOLD. Okay.

Chairman WU. There we go.

Dr. ARNOLD. I will have to apply some intelligence here.

I would like to thank you for the opportunity to discuss NIST's progress in accelerating the development of standards to realize a secure and interoperable nationwide smart grid.

The smart grid is indeed central to the Nation's efforts to increase the reliability, efficiency and security of the electric delivery system and to increase America's use of renewable and distributed clean energy. The smart grid is also an important piece of the Administration's overall goal of fostering innovation and creating millions of jobs in a green energy economy.

As has been said, under the Energy Independence and Security Act of 2007, Congress assigned NIST the primary responsibility to coordinate development of standards for the smart grid. This task represents an enormous challenge and a tremendous opportunity. Several years ago, the National Academy of Engineering described today's electric grid as the greatest engineering achievement of the 20th century. Future generations may well describe the smart grid as the first great engineering achievement of the 21st century. NIST is providing strong national and international leadership to drive the creation of the standards needed to make the smart grid a reality. We are engaging industry, government and consumer stakeholders in an unprecedented open public process.

In April of 2009, NIST launched a three-phase plan to expedite development and adoption of smart grid interoperability standards. I am pleased to tell you that the plan we laid out is on course and on schedule. Phase one of our effort resulted in the January 2010 release of NIST Special Publication 1108, Release 1.0, Framework and Roadmap for Smart Grid Interoperability. It describes a high-level reference model, identifies seven initial standards, specifies 16 priority action plans and the highest priority standards gaps and describes a strategy to establish requirements and standards for smart grid cybersecurity.

The NIST Release 1.0 Framework is also having influence around the world and is being used as a reference by many other countries that are beginning to work on their standards for their smart grid.

Smart grid will ultimately require hundreds of standards, specifications and requirements. Some are obviously needed more urgently than others. To prioritize its work, NIST chose to focus its initial effort on the priorities in FERC's Policy Statement plus additional areas identified by NIST in consultation with DOE [Department of Energy].

The Release 1.0 Framework lays a strong foundation but much work lies ahead. Phase two of the NIST plan saw the establishment of a more permanent public-private partnership, the Smart Grid Interoperability Panel, to guide the development and evolution of the standards. This body is also guiding the establishment of a testing and certification framework for the smart grid which is phase three of the NIST plan.

Cybersecurity is a paramount concern, and this has been the major focus of our effort from the beginning. A NIST-led cybersecurity working group is finalizing a major deliverable that will be published later this month establishing cybersecurity guidelines for the smart grid.

So where are we headed next? Our most immediate priority is completion of the priority action plans we currently have underway. We anticipate that these tasks will result in about 25 additional standards, guidelines and requirements documents to fill the highest priority gaps in the standards post office, and significant progress is being made in these action plans.

Another key priority for NIST is supporting future FERC rule-making to adopt smart grid standards, and NIST has been working very closely with FERC and will continue to do so, and we are also reaching out to state commissions.

I would like to conclude by mentioning some of the major challenges that we are addressing. First is ensuring that our standards are, wherever possible, harmonized internationally. To achieve this, we are fully engaged in all the relevant international standards bodies and in bilateral and multilateral discussions with our governmental counterparts in other countries. Second, we are working to accelerate resolution of some key standards issues that could impede the development of the market if not settled soon, such as communication between consumer appliances in the grid and electric vehicle to grid interconnection. Third, we are continuously weighing the correct balance between speed and deliberation in our work, because any fundamental mistakes made at this stage may be difficult and costly to correct later.

NIST is proud to have been given such an important role and is committed to achieving the Administration's vision. Thank you for the opportunity to testify today. I would be happy to answer any questions that you may have.

[The prepared statement of Dr. Arnold follows:]

### **Introduction**

Chairman Wu, Ranking Member Smith, and Members of the Subcommittee, I am George Arnold, the National Coordinator for Smart Grid Interoperability at the Department of Commerce's National Institute of Standards and Technology (NIST).

Thank you for the opportunity to appear before you today to discuss NIST's progress in accelerating the development of standards needed to realize a secure and interoperable nationwide Smart Grid. I last testified about our progress and plans before the Subcommittee on Environment and Energy on July 23, 2009. Today I would like to update you on what we have accomplished since then, where we are going, and some of the key issues on the horizon that we are addressing.

The Smart Grid, which will modernize the United States electric power delivery system, is central to the Nation's efforts to increase the reliability, efficiency and security of the electric delivery system and also to help build the infrastructure that will facilitate clean, energy sources to American homes and businesses: The Smart Grid utilizes advanced information and communications technologies to replace the one-way flow of electricity and information in the current grid with a two-way flow of electricity and information. This marriage of energy and information technologies will create capabilities to integrate solar, wind, and other forms of renewable energy, enable widespread use of distributed energy sources, provide consumers with tools to reduce energy usage and potentially save money, make the grid more efficient by reducing peak demand, and facilitate electrification of vehicles.

The Smart Grid is an important piece of the Administration's overall goal of fostering innovation and creating millions of jobs in a green economy through the creation of whole new industries and green entrepreneurs. NIST's mission to advance innovation and U.S. industrial competitiveness fits perfectly with this goal and we're committed to helping make that vision a reality.

Modernizing and digitizing the nation's electrical power grid—the largest interconnected machine on Earth—is an enormous challenge and a tremendous opportunity. Several years ago, the National Academy of Engineering described the electric grid as the greatest engineering achievement of the 20th century, and the largest industrial investment in the history of humankind. The basic structure of the present grid has changed little over its hundred-year history. The U.S. grid, which is operated by over 3100 electric utilities using equipment and systems from hundreds of suppliers, has historically not had much emphasis on standardization and thus incorporates many proprietary interfaces and technologies that result in the equivalents of stand-alone silos.

Transforming this infrastructure into an interoperable system capable of supporting the nation's vision of extensive distributed and renewable resources, energy efficiency, improved reliability and electric transportation may well be described by future generations as the first great engineering achievement of the 21st century.

### **NIST's Standards Role: A Framework for Interoperability**

Moving towards nationwide North American, interoperable and secure Smart Grid cannot be done without establishing standards that are, preferably, harmonized with international standards. Under the Energy Independence and Security Act of 2007 (EISA), Congress assigned the National Institute of Standards and Technology (NIST) the "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of Smart Grid devices and systems . . ." [EISA Title XIII, Section 1305]. The act further specifies that the interoperability framework should be "flexible, uniform, and technology neutral." The law also instructs that the framework should accommodate "traditional, centralized generation and distribution resources" while also facilitating incorporation of new, innovative Smart Grid technologies, such as distributed and renewable energy resources and energy storage.

There is an urgent need to establish protocols and standards for the Smart Grid. Deployment of various Smart Grid elements, including smart sensors on distribution lines, smart meters in homes, and widely dispersed sources of renewable energy, is already underway and will be accelerated as a result of Department of Energy (DOE) Smart Grid Investment Grants and other incentives, such as loan guarantees for renewable energy generation projects. Without standards, there is the potential for technologies developed or implemented with sizable public and private investments to become obsolete prematurely or to be implemented without measures necessary to ensure security.

NIST is providing strong national and international leadership to drive the creation of interoperability standards needed to make the Smart Grid a reality. We are

engaging industry, government, and consumer stakeholders in an unprecedented, open, public process. As I will detail shortly, in January of this year the NIST-led process reached a major milestone with the publication of the Release 1.0 Framework and Roadmap for Smart Grid Interoperability (NIST Special Publication 1108). This document provides the initial foundation for an interoperable and secure Smart Grid and has been widely praised by the Smart Grid stakeholder community. It has also provided direction for Smart Grid efforts around the world.

### **Comparatively Speaking: Off to a Fast Start**

We are calling this framework “Release 1.0” because, while it provides a very comprehensive foundation for the Smart Grid, our work to develop the standards is far from complete. A similar effort to develop foundational standards for the Next Generation Networks (NGN) in the telecom domain—the broadband networks we use today to provide integrated telephone, television and internet services—took two years to develop their “Release 1.0” and five years to develop “Release 2.0”. With the Smart Grid we have accomplished in about a year what took two years to do for the NGN. This is in spite of the fact that the Smart Grid is a far more complex system. The fast pace reflects the intensity and urgency with which we and our partners are working.

While we are driving this program with a strong sense of urgency, we must also keep in mind that the foundation we lay with these standards likely will establish the basic architecture of the grid for the next 100 years. Any fundamental mistakes made at this stage may be difficult and costly to correct later. We especially cannot afford to make incorrect architectural choices or adopt weak standards that would compromise the security, reliability or stability of the grid. We need to work both quickly and carefully.

### **Accomplishments**

In April 2009, NIST launched a three-phase plan to expedite development and promote widespread adoption of Smart Grid interoperability standards. This plan was developed after consulting with numerous stakeholders in industry, the standards community, and Federal and state government. The plan, which I described in my testimony last July, reflects the need to rapidly establish an initial set of standards, while providing a robust, well governed process for the evolution of smart grid standards. I am pleased to tell you that the plan we laid out is on course and on schedule.

In May 2009, U.S. Secretary of Commerce Gary Locke and U.S. Secretary of Energy Steven Chu chaired a meeting of nearly 70 executives from the power, information technology, and other industries at which the executives expressed their commitment to support NIST’s plan.

#### *Initial Framework*

In Phase one, we engaged over 1,500 stakeholders representing hundreds of organizations in a series of public workshops over a six-month period. In a recent letter, the U.S. Chamber of Commerce commended NIST for its “willingness to reach out to the private sector on these issues.” The Chamber described the NIST-led process as “transparent and inclusive.”

Through this process, we and our collaborators created a high-level architectural model for the Smart Grid, analyzed use cases, identified applicable standards, determined gaps in currently available standards, and agreed on priorities for new standardization activities. The result of this phase, “NIST Special Publication 1108—NIST Framework and Roadmap for Smart Grid Interoperability Release 1.0,” was published in January 2010.

The Release 1.0 Framework describes a high-level conceptual reference model for the Smart Grid, identifies 75 existing standards that are applicable to the ongoing development of the Smart Grid, specifies 16 high-priority gaps and harmonization issues for which new or revised standards and requirements are needed, documents action plans by which designated standards-setting organizations (SSOs) are addressing these gaps, and describes the strategy to establish requirements and standards to help ensure Smart Grid cyber security.

The Smart Grid is a complex system of systems for which a common understanding of its major building blocks and how they interrelate must be broadly shared. The reference model described in the Release 1.0 Framework provides a foundation to ensure alignment among the many Standards Setting Organizations that are working with NIST on achieving the Smart Grid vision.

The Smart Grid will ultimately require hundreds of standards, specifications, and requirements. Some are needed more urgently than others. To prioritize its work, NIST chose to focus initially on standards needed to address the priorities identified in the Federal Energy Regulatory Commission (FERC) Policy Statement, plus additional areas identified by NIST. The eight priority areas are:

- Demand Response and Consumer Energy Efficiency
- Wide-Area Situational Awareness
- Energy Storage
- Electric Transportation
- Advanced Metering Infrastructure
- Distribution Grid Management
- Cyber Security
- Network Communications

Many of the standards identified by NIST are mature and already widely used by industry, others require revisions to accommodate Smart Grid applications and requirements, and still others are in the draft stage and not yet publicly available. Collectively, these 75 standards provide an extensive foundation for the Smart Grid. They address such issues as standardizing the data captured by smart meters, common information models for the grid, protocols for communicating price and demand response signals between the grid and smart appliances, and the interface between plug-in electric vehicles and the grid for charging at 110 or 220 volts, to provide a few examples. However, there are many gaps in the standards portfolio that must be filled in.

Through the NIST workshops, NIST determined that many potentially useful standards will require revision or enhancement before they can be implemented to address Smart Grid requirements. In addition, stakeholders identified gaps requiring entirely new standards to be developed. In all, a total of 70 such gaps or related issues were initially identified. Of these, NIST selected 16 for which resolution is most urgently needed to support one or more of the Smart Grid priority areas. For each, an action plan involving relevant stakeholders was launched. These Priority Action Plans specify organizations that have agreed to accomplish defined tasks with specified deliverables. One key action plan, to develop a standard to ensure software upgradeability of the millions of smart meters that will be deployed over the next several years, has already been completed. Substantive progress has been made in meeting the milestones of other action plans addressing gaps in the standards portfolio.

#### *Establishing a New Partnership to Maintain Momentum*

Phase two of the NIST plan saw the establishment of a more permanent public-private partnership, the Smart Grid Interoperability Panel (SGIP), to guide the development and evolution of the standards. This body is also guiding the establishment of a testing and certification framework for the Smart Grid, which is Phase three of the NIST plan. The SGIP was formalized and launched in November 2009 and is now in execution mode. During its eight months in existence, membership in the SGIP has grown to over 580 organizations, representing private companies, universities, research institutes, industry associations, standards setting organizations, testing laboratories, and government agencies at the Federal, state and local levels. Nearly 1600 individuals who participate in the committees, working groups, and priority action plans working under the panel, represent these hundreds of organizations. An elected 27-member governing board representing 22 different stakeholder groups ranging from electric utilities, electric equipment manufacturers, building automation providers, information and communications technology companies, state regulators, and even venture capital firms oversees the SGIP. Membership in the SGIP is open to international participants, and 52 organizations from other countries around the world participate in its work. This is helping to ensure that standards used for the Smart Grid in the U.S. are based wherever possible on international standards that are harmonized globally. This provides a double benefit to the U.S. It enables Smart Grid suppliers to cost-effectively address the global market, and it promotes greater supplier competition, which in turn reduces costs for utilities and consumers.

#### *Cyber Security: A Paramount Concern from the Very Beginning*

Cyber security of the Smart Grid is a paramount concern, and this has been a major focus of our effort. A NIST-led cyber security working group, consisting of

over 460 participants from the private and public sectors, is leading the development of a cyber security strategy and guidelines for the Smart Grid. The working group has developed an overall cyber security strategy; selected and revised security requirements for the Smart Grid; identified vulnerability classes and specific cyber security issues applicable to the Smart Grid; performed a privacy impact assessment; specified research and development topics; and is assessing relevant standards and developing a security architecture linked to the Smart Grid conceptual reference model. Results of the group's work have been published in two drafts of *NIST Interagency Report 7628 (Smart Grid Cyber Security Strategy and Requirements)*, issued in September 2009 and February 2010, which have gone through public review. This draft is now being finalized addressing all comments received and will be published as NIST IR 7628: *Guidelines for Smart Grid Cyber Security* in July of this year.

### Where Are We Headed

Our most immediate priority is completion of the Priority Action Plans that are now tackling the highest-priority needs in the standards portfolio. One action plan, the Smart Meter Upgradeability Standard, has already been completed. The other Priority Action Plans currently underway are:

- Data standard for consumer energy usage information
- Common specification for communicating electricity price and product definition
- Common scheduling mechanism for energy transactions
- Common information model for distribution grid management
- Standard demand response signals
- DNP3 Mapping to IEC 61850 Objects
- Harmonization of IEEE C37.118 with IEC 61850 and precision time synchronization
- Transmission and distribution power systems models mapping
- Guidelines for use of the Internet Protocol suite in the Smart Grid
- Guidelines for use of wireless communications in the Smart Grid
- Energy storage interconnection guidelines
- Interoperability standards to support plug-in electric vehicles
- Standard meter data profiles
- Harmonize power line carrier standards for appliance communications in the home
- Standards for Wind Plant Communication

One action plan I wish to highlight is the work to create a standard for consumer energy usage information. Today, the only information available to most consumers about their electricity usage is their monthly utility bill. Consumers need more timely and detailed electronic access to their data in order to reduce energy usage. Under the NIST action plan, the North American Energy Standards Board is developing a standard that will define the data on energy usage that smart meters and utility information systems must make available to consumers. A draft of this standard will be available by the end of 2010. As these highest priority action plans are completed in 2010, new action plans will be launched by the Smart Grid Interoperability Panel to address additional gaps that still need to be filled, as well as new requirements and technologies that emerge.

Another high priority for NIST is supporting the forthcoming FERC rulemaking. EISA directs FERC to institute a rulemaking proceeding to adopt such standards and protocols as may be necessary to ensure smart-grid functionality and interoperability in interstate transmission of electric power, and regional and wholesale electricity markets, at any time after NIST's work has led to sufficient consensus in the Commission's judgment. NIST has been working very closely with FERC throughout the entire process.

The evolving nature of the Smart Grid implies that the regulatory adoption of standards will be an ongoing process rather than a one-time action. Therefore I anticipate that FERC's initial rulemaking will focus on a subset of the standards identified by NIST that are the most mature and the most critically needed for end-to-end Smart Grid interoperability and security. NIST, working closely with FERC staff, is preparing additional technical documentation and analysis of these standards to inform FERC's decision about which standards to include in its initial rulemaking. NIST is working to complete these documents by the end of July.

It is important for Federal and state regulators to keep in mind, when considering the adoption of standards, that while all of the standards identified through the NIST process are needed for the Smart Grid, it is not necessary or appropriate for all of them to be adopted in regulations. Many consensus standards are already widely used by industry on a strictly voluntary basis. In some cases their adoption in regulations can be counterproductive. A careful balance must be struck to ensure that the most critical standards needed to ensure end-to-end interoperability and security are adopted in regulations, without impeding continuing innovation and technology improvement.

Another major priority is the establishment of a testing and certification framework for the Smart Grid. The standards specifications are necessary but not sufficient to ensure interoperability and security. A robust and well-defined testing and certification program is needed.

A new Testing and Certification Committee that has been established under the Smart Grid Interoperability Panel is guiding the development of a testing and certification framework for the Smart Grid. This committee is co-chaired by a leading expert from the private sector and a manager in the NIST Office of the National Coordinator for Smart Grid Interoperability. The committee includes representatives of leading testing laboratories, industry associations, electric utilities, and smart grid suppliers. The committee is working to prioritize the types of interoperability testing needed, laboratory qualification criteria, and requirements for Testing Organizations and Certification Organizations to successfully facilitate conformity assessment to product or system interoperability and cyber security standards.

There are few formalized test programs currently in existence focused on the Smart Grid. One of the most urgent areas of need is a formalized program to test the conformance of smart meters against applicable Smart Grid cyber security requirements and standards. NIST is using a portion of its Recovery Act funds to develop a smart meter cyber security conformance program. A solicitation for a private sector contractor to support NIST in developing this program closed on June 10, 2010, and our goal is to have the initial test methodology developed and ready for deployment within 12 months from the contract award date.

### **Challenges and Opportunities**

The task of developing standards for an infrastructure like the Smart Grid is a large and complex undertaking; however, it is eminently doable. There have been several previous infrastructure standards projects of similar magnitude that were accomplished successfully and with which I have personal experience.

Thirty years ago, Bell Laboratories successfully put in place architecture for the complete automation of maintenance and operations in the nationwide telecommunications network, with an underlying foundation of protocols and standards that utilized distributed computing and data networking technology of that era. That job was comparable in scale to the current challenge of the Smart Grid; however the coordination challenge was a bit easier because the national network at that time was owned and operated by a single entity with a captive manufacturer rather than 3100 utilities and hundreds of suppliers.

The evolution of the Internet provides another example of a global infrastructure that has evolved over the course of decades, using open standards to achieve interoperability in a flexible way to support new applications and technologies that were never imagined at the outset. Like the Internet, the Smart Grid will need to evolve over the 15–20 years in which its deployment will likely occur, and in that sense the development of the standards will be an ongoing process.

One of the key challenges that we face is to ensure that our standards are, wherever possible, harmonized internationally. This provides a double benefit. It ensures the broadest possible market for U.S. Smart Grid suppliers, helping U.S. companies export their smart grid products, technologies, and services overseas, while creating high technology and jobs within the United States. The Administration's National Export Initiative (NEI) aims to double U.S. exports in five years, with the goal of creating two million new jobs in the United States. Smart Grid companies and technology providers based in the United States will be instrumental in advancing Smart Grid deployment in overseas markets while creating jobs at home. This will support NEI's efforts on international standards, promote greater supplier competition, and lower equipment prices for utilities and consumers. Our policy has been to base our U.S. Smart Grid on international standards wherever possible. Of the 75 standards identified in the NIST Release 1.0 Framework, 77 percent are produced by international standards organizations.

The U.S. is ahead of every other country in establishing a standards framework for its Smart Grid. We have intentionally opened our process to the international

community and expressed a preference for international standards to encourage harmonization. We have also invested significant effort in establishing bilateral and multilateral dialogs with other nations that are working on Smart Grids, including Canada, Mexico, Brazil, the EU (and many of its member states), Japan, Korea, Australia, India and China. It will not be possible to harmonize all our standards, given the historical differences that exist between electrical systems in different parts of the world, but we are making harmonization a very high priority.

China in particular is making very large investments to create a Smart Grid, with significant emphasis on transmission and distribution infrastructure. By one estimate, China will spend \$10 billion annually on Smart Grid/smart infrastructure systems. There is great opportunity for foreign investment. Companies that specialize in transmission and transformation equipment, automation equipment, and information and communications technology components are well-positioned to contribute to China's grid development projects. I have read some reports that predict that China's preference for indigenous innovation will extend to the Smart Grid, and that China may seek to establish its own standards for the Smart Grid in the belief that the size of its market will lead to their adoption as de facto global standards. I hope that this will not be the case, and that China will take action to strengthen collaboration with the U.S. in creating harmonized international standards.

Another challenge that we face is accelerating the resolution of some key standards issues that could impede development of the market if not settled soon.

Several major appliance manufacturers have announced their intention to bring to market Smart Grid-enabled consumer appliances beginning in late 2011, provided that standards for communication between appliances and the grid for pricing and demand response signals are resolved by the end of 2010. The existence of too many competing standards has the potential to fragment the market and impede its development. Recognizing the urgency, a task group of the SGIP Governing Board including representatives from the appliance, consumer electronics, electric utility, building automation, and IT industries, and other stakeholders including state regulators, has been addressing the issue. In conjunction with a related effort being undertaken by the Association of Home Appliance Manufacturers, we are on target to achieve a timely resolution of the standards for smart appliances to communicate with the grid to meet the needs of the appliance industry.

Another issue that will be more difficult to resolve is the interconnection standard between electric vehicles and the grid for high-voltage, rapid charging. As I indicated earlier, the standards for charging at 110 or 220 volts have been settled and this will support the deployment of first generation electric vehicles. Charging stations that support rapid charging in minutes rather than hours will be needed, however, for widespread adoption of electric vehicles. There are at least four different competing proposals advocated by auto manufacturers headquartered in the U.S., Japan, Europe and China on what this interface should be. Lack of clarity on what the standard will be could impede development of a charging infrastructure in the U.S. Our Priority Action Plan on electric vehicles includes the timely resolution of this difficult issue as a key goal.

An overarching challenge that we face in setting standards for the Smart Grid is ensuring that they are sufficiently flexible to preserve options for the evolution of the grid as we gain experience with early deployment. The fact is that there are still many unknowns in such issues as the degree of centralized vs. distributed control of the grid. For example as we move toward more distributed renewable generation, with households and buildings not only consuming power but also generating power and selling it back into the grid, and appliances behaving in different ways in response to price signals, having effective controls to ensure stability of the grid will become increasingly important. New, more dynamic measurements and models of grid performance will be needed. Measurements, characterization, and models of storage devices, electric vehicles, and distribution system loads have to be developed. These are areas in which NIST's expertise in measurement science can contribute and we are addressing them in the program planning for our research efforts related to the Smart Grid. Cyber security will remain a significant challenge as threats continue to evolve, and application of NIST's expertise in computer and network security to the Smart Grid will continue to be a top priority.

Finally, I would like to mention an opportunity. Basing the Smart Grid architecture on open standards, as we are doing, may facilitate multi-use scenarios, in much the same way as the Internet has evolved over time to provide a common set of protocols and standards supporting voice, video and data applications. Japan, which is following what we are doing very closely, is moving in this direction. Japan has recently unveiled their national Smart Grid program, which they have called the "Smart Community". Their roadmap envisions a common architecture supporting automation in their electric grid, water and gas networks, energy efficient buildings,

and intelligent transportation. I believe that the architecture and standards for the U.S. Smart Grid should consider this broader concept and not limit our future direction.

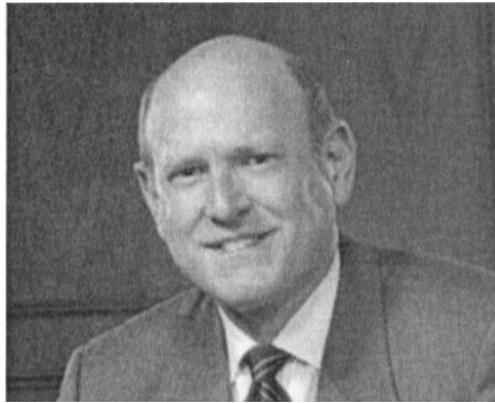
The knowledge gained by rigorous analysis of the performance of the Smart Grid under the Department of Energy's (DOE) ARRA programs will give us valuable information to determine whether or not benefits could be gained by applying the standards based intelligence infrastructure to other domains important to our society.

### Conclusion

The Smart Grid, with the unique investment opportunity afforded by the American Recovery and Reinvestment Act, represents a once in a lifetime opportunity to renew and modernize one of the Nation's most important infrastructures. NIST is proud to have been given such an important role and is committed to achieving the Administration's vision of a cleaner, more reliable, more efficient and effective electricity grid that creates jobs and reduces our dependence on others.

Thank you for the opportunity to testify today on NIST's work on Smart Grid interoperability. I would be happy to answer any questions you may have.

### BIOGRAPHY FOR GEORGE W. ARNOLD



George Arnold was appointed National Coordinator for Smart Grid Interoperability at the National Institute of Standards and Technology (NIST) in April 2009. He is responsible for leading the development of standards underpinning the nation's Smart Grid. Dr. Arnold joined NIST in September 2006 as Deputy Director, Technology Services, after a 33-year career in the telecommunications and information technology industry.

Dr. Arnold served as Chairman of the Board of the American National Standards Institute (ANSI), a private, non-profit organization that coordinates the U.S. voluntary standardization and conformity assessment system, from 2003 to 2005. He served as President of the IEEE National Coordinator for Smart Grid Standards Association in 2007-08 and is currently Vice Interoperability Office of the Director President-Policy for the International Organization for Standardization (ISO) where he is responsible for guiding ISO's strategic plan.

Dr. Arnold previously served as a Vice-President at Lucent Technologies Bell Laboratories where he directed the company's global standards efforts. His organization played a leading role in the development of international standards for Intelligent Networks and IP-based Next Generation Networks. In previous assignments at AT&T Bell Laboratories he had responsibilities in network planning, systems engineering, and application of information technology to automate operations and maintenance of the nationwide telecommunications network.

Dr. Arnold received a Doctor of Engineering Science degree in Electrical Engineering and Computer Science from Columbia University in 1978. He is a Senior Member of the IEEE.

Chairman WU. Thank you very much, Dr. Arnold.  
Mr. Emmett, please proceed.

**STATEMENT OF MR. MASON W. EMNETT, ASSOCIATE DIRECTOR OF THE OFFICE OF ENERGY POLICY AND INNOVATION, FEDERAL ENERGY REGULATORY COMMISSION**

Mr. EMNETT. Thank you, Mr. Chairman and Members of the Subcommittee. My name is Mason Emnett and I am the Associate Director of the Office of Energy Policy and Innovation at the Federal Energy Regulatory Commission. Yes, that is a mouthful. I appear today before you as a staff witness. My testimony does not necessarily represent the views of the Commission or any individual commissioner.

As Dr. Arnold explained, the Commission shares statutory responsibility regarding the development of smart grid interoperability standards with the National Institute of Standards and Technology. The Energy Independence and Security Act of 2007 directs NIST to coordinate the development of a framework to achieve interoperability of smart grid systems and devices. Once the Commission is satisfied that NIST's work has led to sufficient consensus, the Commission is directed to institute a rulemaking proceeding to adopt such standards and protocols as may be necessary to ensure smart grid functionality and interoperability in the interstate transmission of electricity and in regional and wholesale electric markets.

In order to provide input to NIST in the development of its interoperability framework, the Commission in July 2009 issued a smart grid policy statement that identified areas that deserved high priorities in the smart grid standards development process. The Commission explained that addressing these issues would help expedite the development of functions that are important to Federal energy policy. NIST embraced the Commission's priority in preparing its framework, which was released by NIST in January 2010 and included additional priorities identified by NIST. The NIST framework identifies an initial set of 75 interoperability standards that are applicable or are likely applicable to the ongoing development of smart grid technologies and applications. The framework also outlines a number of action plans providing for further standards development to address the priorities identified by NIST and the Commission.

As Dr. Arnold mentioned, to provide continuing stakeholder input in the smart grid standards development process, NIST has formed the Smart Grid Interoperability Panel, a public-private partnership of stakeholder groups supporting NIST in the ongoing coordination, acceleration and harmonization of standards development for the smart grid. Although the Commission is not a formal member of the interoperability panel or its governing board, our staff has attended meetings of both as well as many meetings regarding work on the priority action plans and working group meetings focusing on such issues as cybersecurity.

With regard to the adoption of smart grid standards by the Commission, the commission explained in the Policy statement that its statutory mandate under EISA [Energy Independence and Security Act] requires it to consider standards that will be applicable to all electric power facilities with smart grid features. This could include facilities at the local distribution level and those used directly by retail customers as long as the related standard is necessary for

the purpose identified in EISA. The Commission stated, however, that it would not adopt a smart grid standard without a demonstration of sufficient cybersecurity protection. The Commission noted in the policy statement that adoption by the Commission of a standard under EISA does not make the standard mandatory. To the extent the Commission might wish to make any particular smart grid standard mandatory, its authority to do so must derive under other statutory authority such as the Federal Power Act. The Commission also explained that adoption of a smart grid standard by the Commission under EISA does not alter any state jurisdiction that may exist with regard to compliance with the smart grid standard.

To support an active dialog with states regarding the interest in smart grid development, the Commission has formed a Federal-state collaborative with the National Association of Regulatory Utility Commissioners and encouraged states to actively participate in the smart grid standards development process.

Finally, the Commission also has sought to encourage the development of smart grid applications by providing rate incentives to early adopters of smart grid technologies. The Commission expressed concern that waiting for all technical issues to be resolved before beginning investment in smart grid deployment would frustrate the development of smart grid standards. The Commission will therefore allow recovery of a jurisdictional smart grid cost prior to finalization of related smart grid standards if certain specific demonstrations are made.

In conclusion, the Commission remains committed to supporting development of smart grid standards and investments in smart grid technologies where appropriate. Continued cooperation among NIST, other Federal agencies, state regulators and industry representatives as well as consumer representatives and other interested entities will enable the successful deployment of innovative, effective and secure smart grid technologies.

Thank you again for the opportunity to appear before you today. I would be happy to answer any questions you may have.

[The prepared statement of Mr. Emnett follows:]

PREPARED STATEMENT OF MASON W. EMNETT

Mr. Chairman and members of the Subcommittee:

My name is Mason Emnett, and I am the Associate Director of the Office of Energy Policy and Innovation at the Federal Energy Regulatory Commission (Commission). I appear before you as a staff witness; my testimony does not necessarily represent the views of the Commission or any individual Commissioner. Thank you for the opportunity to appear before you today to discuss the progress of standards development towards smart grid interoperability and modernization of the nation's electricity transmission and distribution system.

The Chairman of the Commission, Jon Wellinghoff, most recently testified about the benefits of smart grid technologies and the status of the agency's work on smart grid standards on March 23, 2010, before the Energy and Environment Subcommittee of the House Committee on Energy and Commerce. Today, I will focus on the Commission's efforts to support the development of smart grid standards, its role in adopting standards, and its work to incentivize investment in smart grid technologies.

**Development of Smart Grid Standards**

In the Energy Independence and Security Act of 2007 (EISA), Congress enacted several requirements related to development of a smart grid. Among other things,

EISA directs the National Institute of Standards and Technology (NIST) to coordinate the development of a framework to achieve interoperability of smart grid devices and systems. In furtherance of this responsibility, NIST has engaged in significant outreach to identify standards for potential inclusion in a smart grid interoperability framework, leading to the publication in January 2010 of the Framework Roadmap for Smart Grid Interoperability Standards, Release 1.0 (Framework).

To provide input into the development of the NIST Framework, the Commission in July 2009 issued a Smart Grid Policy Statement that, among other things, discussed smart grid functions and characteristics that could help address challenges to the reliable operation of the transmission system. In response to the need for action on these challenges, the Commission identified areas that deserved high priority in the smart grid standards development process. These areas include two cross-cutting issues, system security and inter-system communication, and four key grid functionalities: wide-area situational awareness, demand response, electric storage and electric vehicles.

The Commission explained that addressing these priorities would help to expedite the development of functions that are important to Federal energy policy. For example, wide-area situational awareness will provide tools that can improve reliability. Demand response and electric storage will support initiatives that have emerged in many states such as integrating renewable generation to permit utilities to meet state-mandated renewable portfolio standard requirements. Electric vehicles will help reduce our dependence on foreign oil, and will also have favorable environmental impacts. NIST embraced these priorities in drafting its Framework, and added two additional priorities for standards: advanced metering and distribution system automation.

In order to ensure broad support for these priorities, staff from NIST and the Commission have engaged in individual and coordinated outreach with standards development organizations from the telecommunications, internet, and power industries to discuss framework development and the respective roles of each agency in the standards development process. NIST also released a draft of its Framework in September 2009 to provide an opportunity for public comment and collaboration with the Commission prior to finalizing the document. Based on this feedback, NIST's Framework identified 75 interoperability standards that are applicable, or are likely applicable, to the ongoing development of smart grid technologies and applications. The NIST Framework also outlines the priority areas identified by both the Commission and NIST in the smart grid standards development process. In particular, sixteen Priority Action Plan areas were created to address gaps in standards that are critical for the interoperability of the smart grid.

In addition, NIST has provided for continuing stakeholder input into the smart grid standards development process through formation of the Smart Grid Interoperability Panel (SGIP), a public-private partnership of 22 stakeholder groups supporting NIST in the ongoing coordination, acceleration and harmonization of standards development for the smart grid. The Governing Board of this Panel was elected and tasked with maintaining a broad perspective regarding the NIST interoperability framework and providing recommendations to NIST. Within the SGIP are two standing committees and one permanent working group to support NIST on particular issues. One standing committee has responsibility for outlining the architecture needed to realize the smart grid vision. The second committee addresses testing and certification of vendor products and systems for conformance with smart grid standards and for interoperability.

The working group within the SGIP addresses matters related to the security of the smart grid, including reviewing standards to determine the level of cyber security present and determining whether each identified standard meets appropriate security requirements. This working group has released two drafts of an Interagency Report on Smart Grid Cyber Security Strategy and Requirements in September 2009 and February 2010, and is currently reviewing comments on the latest draft. The report addresses risks, vulnerabilities, threats, and impacts, and provides guidance related to smart grid cyber security.

Although the Commission is not a formal member of the SGIP or its Governing Board, Commission staff has attended meetings of both, as well as many meetings regarding work on the Priority Action Plans. Commission staff is also actively involved in the work of the cyber security working group, as the Commission recognizes that inadequate cyber security could threaten the health of the bulk power system.

### Adoption of Standards by the Commission

As defined by EISA, the Commission's responsibility to review a smart grid interoperability standard is triggered once the Commission is satisfied that NIST's work has led to sufficient consensus. At such time, the Commission is directed to institute a rulemaking proceeding to adopt such standards and protocols as may be necessary to ensure smart grid functionality and interoperability in interstate transmission of electric power and regional and wholesale electric markets.

The Commission explained in the Policy Statement that it understood this mandate to give it authority to adopt a standard that will be applicable to all electric power facilities and devices with smart grid features, including those at the local distribution level and those used directly by retail customers, as long as the standard is necessary for the purpose identified in EISA. The Commission noted, for example, that two-way communications are a distinguishing characteristic of smart grid devices on both the transmission and distribution systems. Such two-way communication capability is essential to the smart grid vision of interoperability, allowing the transmission and distribution systems to communicate with each other and affecting the security and functionality of each other. Consequently, the Commission found that EISA grants it the authority to adopt standards that relate to distribution facilities and devices deployed at the distribution level, if the Commission finds that such standards are necessary for smart grid functionality and interoperability in interstate transmission of electric power, or in regional and wholesale electric markets.

In addition, the Commission stated in the Policy Statement that it will require a demonstration of sufficient cyber security protection for a standard to be adopted. This consideration is consistent with EISA's inclusion of cyber security as a characteristic of a smart grid,<sup>1</sup> EISA's identification of cyber security as a "smart grid function,"<sup>2</sup> and EISA's requirement for the Department of Energy (in consultation with the Commission, the Department of Homeland Security, and the Electric Reliability Organization certified by the Commission) to study and report on the potential impact of deployment of Smart Grid systems on the security of the Nation's electricity infrastructure.<sup>3</sup>

The Commission noted in the Policy Statement, however, that adoption by the Commission of a standard under EISA does not make the standard mandatory, nor does EISA give the Commission authority to require the development of a smart grid standard. To the extent the Commission might wish to make any smart grid standards mandatory, its authority to do so must derive from other statutory authority, such as the Federal Power Act. For example, the Commission has the authority under section 215 of the Federal Power Act to approve and enforce reliability standards developed by the North American Electric Reliability Corporation. The Commission also has the authority under sections 205 and 206 of the Federal Power Act to establish the rates, terms and conditions of wholesale sales and interstate transmission of electricity, including the incorporation into Federal regulations of business practice standards developed by the North American Energy Standards Board. Although there is the potential for some overlap in the adoption of smart grid standards under EISA and review of reliability or business practice standards under the Federal Power Act, these sources of jurisdiction are distinct and the Commission has interpreted EISA as not changing the scope of its jurisdiction.

The Commission also explained in the Policy Statement that adoption of a smart grid standard by the Commission under EISA does not alter any state jurisdiction that may exist to require compliance with smart grid standards. To that end, the Commission has recognized that states have an interest in the functionalities of smart grid technologies and encouraged states to actively participate in the standards development process to ensure that their perspectives are represented. The Commission expressed in the Policy Statement an expectation that its adoption of national standards should enhance, not limit, the policy choices available to each state.

To support an active dialogue with the states on these issues, the Commission has formed a Federal-state collaborative with the National Association of Regulatory Utility Commissioners to address issues related to smart grid and demand response. This body has received substantial input from a variety of smart grid stakeholders on a range of issues, including smart grid interoperability standards, consumer access to and privacy of data, potential smart grid benefits, and potential new business models and regulatory approaches. By coordinating consideration of these

<sup>1</sup> EISA section 1301(2).

<sup>2</sup> EISA section 1306(d)(5).

<sup>3</sup> EISA section 1309(b).

issues, the Collaborative provides a forum to identify how smart grid development can benefit consumers and to address the concerns of regulators regarding grid security and functionality.

### **Incentivizing Smart Grid Investment**

The Commission also has sought to encourage the development of smart grid applications by providing rate incentives to early-adopters of smart grid technologies. In its Policy Statement, the Commission established an interim rate policy to apply during the period prior to adoption of interoperability standards by the Commission. The Commission expressed concern that waiting for all technical issues to be resolved before beginning investment in smart grid deployment would frustrate the development of smart grid standards. The Commission concluded that smart grid resources deployed with appropriate protections during the interim period prior to the Commission's adoption of interoperability standards could instead increase our body of knowledge and ultimately assist the standards development process.

During this period, the Commission will allow recovery of Commission-jurisdictional smart grid-related costs if four demonstrations are made. These four demonstrations are (1) the smart grid facilities will advance the policy and goals of section 1301 of EISA, (2) the smart grid facilities will not adversely affect the reliability and cybersecurity of the bulk-power system, (3) the applicant has minimized the possibility of stranded investment in smart grid equipment, and (4) the applicant agrees to provide certain information to the Department of Energy Smart Grid Information Clearinghouse.

With regard to the fourth demonstration, the Commission recognizes the benefit of DOE implementing a Smart Grid Information Clearinghouse to collect information about the results of the smart grid grant and demonstration programs that have been funded by the *American Recovery and Reinvestment Act of 2009*. This information can help Federal and state regulators as they make decisions on smart grid filings from electric utilities, providing knowledge gained from pilot projects, lessons learned about the impact of investments, and best practices. Commission staff has worked with DOE and other stakeholders to help define the precise data that should be collected, and the Commission has sought to supplement that data by requiring applicants for rate recovery of smart grid costs to provide relevant information to the Clearinghouse.

### **Conclusion**

In conclusion, the smart grid effort has benefited from the active participation of many industry segments in NIST's standards development process. The Commission remains committed to continued cooperation among NIST, other Federal agencies, state regulators, industry representatives, consumer representatives, and other interested entities in order to realize the successful deployment of innovative, efficient and secure smart grid technologies.

Thank you again for the opportunity to appear before you today. I would be happy to answer any questions you may have.

#### **BIOGRAPHY FOR MASON W. EMNETT**

Mason Emmett is Associate Director of the Office of Energy Policy and Innovation at the Federal Energy Regulatory Commission. The Office provides leadership in the development and formulation of policies and regulations to address emerging issues affecting wholesale and interstate energy markets.

Mr. Emmett joined the Commission in 2006, serving as Senior Legal Advisor in the Commission's Office of General Counsel. There he advised the Commission on legal and policy matters related to electric transmission service, wholesale power sales, electric system reliability, corporate regulation of public utilities, and enforcement proceedings. Prior to joining the Commission, Mr. Emmett was in private practice with the law firm of Skadden, Arps, Slate, Meagher and Flom LLP in Washington, DC, where he represented public utilities appearing before the Commission on matters related to market design, wholesale rates, mergers and acquisitions, and regulatory compliance.

Mr. Emmett is a graduate of the Georgetown University Law Center and of the University of Texas at Arlington.

Chairman WU. Thank you very much.  
Mr. McDonald, please proceed.

**STATEMENT OF MR. JOHN D. McDONALD, P.E., DIRECTOR OF  
TECHNICAL STRATEGY AND POLICY DEVELOPMENT, GE EN-  
ERGY**

Mr. McDONALD. Good morning, Mr. Chairman and Members of the Subcommittee, I am John McDonald, Director of Technical Strategy and Policy Development with GE's Digital Energy business. Digital Energy provides technology solutions enabling grid management and optimization for electric utilities worldwide. And in my role, I set and drive the vision integrating standards, policy, regulatory and industry participation with customer solutions development.

My comments today are based on over three decades of experience in the electric industry including past President of the Institute of Electrical and Electronics Engineers, or IEEE, Power and Energy Society, current member of DOE's Smart Grid Electricity Advisory Committee, Board Member of the Gridwise Alliance and the IEEE Standards Association, and Governing Board Chair of the NIST Smart Grid Interoperability Panel, or the SGIP.

I welcome this opportunity to update you on the SGIP's efforts to support smart grid architecture and standards and offer GE's perspectives on principles to guide standards development.

The smart grid is essential to addressing our energy demand, security and environmental challenges. We commend our Nation's leadership for embracing the smart grid in the Energy Independence and Security Act of 2007 and the American Recovery and Reinvestment Act [ARRA] of 2009. This legislation and direction from Federal and state regulatory agencies gives our industry a tremendous opportunity to begin transforming our grid into a more automated, interactive, and intuitive power delivery system.

Crucial to this undertaking are system architecture and standards, testing and certification and cybersecurity. These are the foundation for bringing together the electrical and communications infrastructure and for evolving technology to meet many and disparate needs. They also provide a framework for development, a roadmap for progress, and a catalyst for continued industry investment.

Given the importance and complexity of these areas, there is a need for the government to play a coordinating role. The National Institute of Standards and Technology, or NIST, under Dr. George Arnold's leadership as National Coordinator for Smart Grid Interoperability, has embraced this role and is working diligently to ensure we create a foundation that is built to last and a modern grid that is more robust, responsive and resilient.

The SGIP is lead by three core teams—NIST, Plenary officers, and a Governing Board—and is fully supported by an administrator. Our membership is large and diverse by design, as it is free and open to all who share the smart grid vision. To date, it consists of some 1,700 individuals from 590 member organizations representing 22 stakeholder categories. Furthermore, the membership is organized into three standing committees, six domain expert working groups and 16 priority action plan teams, and now supported by a Program Management Office.

Since the beginning of the year, NIST and the SGIP have gained interest and traction worldwide on their Smart Grid Conceptual

Reference Model. The identification and prioritization of the 75 existing standards of greatest impact to smart grid interoperability and our priority action plans to address gaps and inconsistencies are driving much-needed focus while the SGIP structure and operating rhythm are driving much-needed collaboration and consensus. Timelines are being adhered to, even accelerated, in light of related policy discussions and actions. Meetings are being co-located with other stakeholders and industry influencers to further harmonize our respective work.

I would also like to share that GE believes the following principles should guide the government's engagement in private-sector standards activities: number one, encourage consensus-based adoption of technical standards; two, balance Federal leadership with private-sector innovation; three, promote international standards development; four, utilize Federal R&D to support standards development; and five, educate stakeholders to accelerate deployment of standards.

In closing, let me say thank you for your interest in and evaluation of how smart grid architecture and standards are progressing. As these represent the foundation we build upon, that will guide our technology development and innovation for years to come, it is essential that we continue to move forward in a deliberate, disciplined fashion that represents and respects all industry stakeholders. While the work of NIST and the SGIP is extremely challenging, it is always rewarding given we are charting the course for a truly 21st century grid, steady, sustainable and truly smart. Thank you.

[The prepared statement of Mr. McDonald follows:]

PREPARED STATEMENT OF JOHN D. McDONALD

Good morning Mr. Chairman and members of the Committee, I am John McDonald, Director, Technical Strategy and Policy Development, with GE Energy's Digital Energy business. In this role, I set and drive the vision that integrates standards, policy, regulatory and industry participation with customer solutions development at Digital Energy.

My comments today are based upon my more than three decades of experience working in the electric power industry, my position at GE and my numerous industry leadership roles. These include Past President of the Institute of Electrical and Electronics Engineers (IEEE) Power & Energy Society, current member of the Department of Energy (DOE) Smart Grid Electricity Advisory Committee, current Board Member of The GridWise Alliance and the IEEE-SA (Standards Association), and current Chair of the Governing Board of the NIST Smart Grid Interoperability Panel (SGIP).

I welcome this opportunity to provide an update on the SGIP's efforts in support of Smart Grid architecture and standards, and also to offer perspectives on behalf of GE on principles to guide standards development.

**Introduction**

The Smart Grid is essential to addressing the energy demand, security and environmental challenges we face. We commend our nation's leadership for embracing the Smart Grid in the Energy Independence and Security Act (EISA) of 2007 and the American Recovery and Reinvestment Act (ARRA) of 2009.

This legislation, and the direction being provided by various Federal and state regulatory agencies, gives the industry a tremendous opportunity to noticeably begin transforming our grid into a more automated, interactive and intuitive power delivery system.

Crucial to this undertaking are system architecture and standards, the foundation for bringing together the electrical and communications infrastructure and for evolving technology to meet many and disparate needs. System architecture and stand-

ards that foster interoperability provide a framework for development, a roadmap for progress and a catalyst for continued industry investment.

In this area, and the areas of testing and certification and cyber security, there is a need for the government to play a coordinating role. The National Institute of Standards and Technology (NIST), under Dr. George Arnold's leadership as National Coordinator for Smart Grid Interoperability, has embraced this role and is working diligently to ensure we create a foundation that is built to last and a modern grid that will remain one of mankind's greatest achievements.

And, while all stakeholders want to move fast and get it right from the start, the reality is that we need to move with purpose and be able to adapt to a dynamic environment. Flexibility, uniformity and technology neutrality are key considerations for the decisions we make around systems architecture and standards. Furthermore, we need to make those decisions in an open, inclusive, transparent manner, where thoughtful debate, technology innovation and market forces help guide us. So balance—in terms of participation, perspective and direction—is essential to advancing both national and international Smart Grid efforts. To be effective, to realize our vision and produce the outcomes we intend to, the private and public sectors must continue to successfully partner with one another. We are working well today in this new paradigm and we will continue to improve with time.

### **GE Energy**

GE Energy is one of the world's leading suppliers of power generation and energy delivery technologies with businesses focused on fossil power, gasification, nuclear, renewable energy—including wind, solar and biomass, oil and gas, water, as well as transmission and distribution. We have more than 100 years of industry experience, and our team of 65,000 employees operates in more than 140 countries.

### **GE Digital Energy**

GE Digital Energy provides technology solutions that enable grid management and optimization for electric utilities worldwide. These solutions encompass hardware, software and services supporting the entire electricity delivery value chain, from power transformers at the generation switchyard to smart meters at the customer premises. They help utilities boost their productivity and reliability, while at the same time reducing their environmental footprint, and they empower consumers to monitor and control their electricity usage.

We have a strong North American presence, with headquarters in Atlanta, Georgia, and facilities across the United States, as well as in Mexico, Canada, the United Kingdom, Spain, Switzerland and India.

The business has experienced significant growth over the past few years, and we expect this trend to continue as electric utilities worldwide prepare for a more secure, low carbon energy future.

### **The NIST Roadmap<sup>1</sup>**

The NIST Roadmap is phase one of a three-phase plan to establish standards, priorities and a framework to achieve Smart Grid interoperability. The second phase of the plan, in which I am pleased to participate, is the SGIP. The SGIP is an ongoing, public-private organization that provides an open process through which stakeholders can participate in coordinating, harmonizing and accelerating Smart Grid standards development. The third phase of the plan is the establishment of a framework for testing conformity with Smart Grid standards and certifying the compliance of Smart Grid devices and systems.

To help guide the industry, NIST defines interoperability as follows:

The capability of two or more networks, systems, devices, applications, or components to exchange and readily use information—securely, effectively, and with little or no inconvenience to the user.<sup>2</sup> The Smart Grid will be a system of interoperable systems. That is, different systems will be able to exchange meaningful, actionable information. The systems will share a common meaning of the exchanged information, and this information will elicit agreed-upon types of re-

<sup>1</sup>NIST *Framework and Roadmap for Smart Grid Interoperability Standards*, Release 1.0, January 2010.

<sup>2</sup>Recovery Act Financial Assistance, Funding Opportunity Announcement. U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, Smart Grid Investment Grant Program Funding Opportunity Number: DE-FOA-0000058.

sponse. The reliability, fidelity, and security of information exchanges between and among Smart Grid systems must achieve requisite performance levels.<sup>3</sup>

The NIST Roadmap contains several important items that shape the work of the SGIP.

- A conceptual reference model . . . to present a shared view of Smart Grid's complex system of systems and to facilitate design of Smart Grid architecture (See Figure 1)
- An initial set of 75 Smart Grid standards for implementation . . . to address issues identified by NIST and priorities identified in the Federal Energy Regulatory Commission (FERC) Smart Grid Policy Statement<sup>4</sup>—demand response and consumer energy efficiency, wide-area situational awareness, energy storage, electric transportation, advanced metering infrastructure, distribution grid management, network communications and cyber security
- Priorities for developing additional standards and making revisions to existing standards, with supporting action plans . . . to resolve major gaps affecting interoperability and security of Smart Grid components
- Initial steps toward a Smart Grid cyber security strategy . . . to assess risks and to identify requirements to address those risks

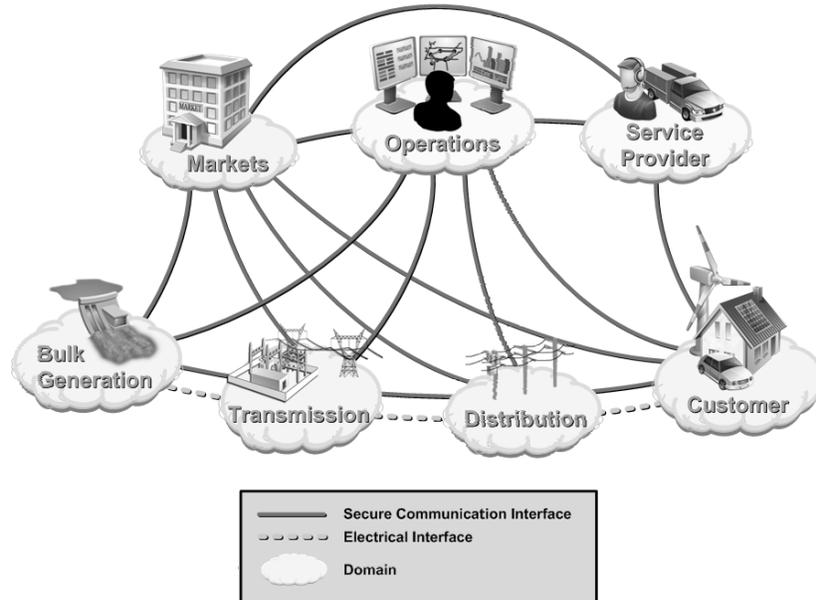


Figure 1 – NIST Smart Grid Conceptual Reference Model

#### Smart Grid Interoperability Panel<sup>5</sup>

Initiated by NIST and established in November 2009, the SGIP is dedicated to the interoperability of Smart Grid devices and systems. According to the SGIP charter:

The Smart Grid Interoperability Panel is a membership-based organization created by an Administrator under a contract from NIST to provide an open proc-

<sup>3</sup>GridWise Architecture Council, *interoperability Path Forward Whitepaper*, November 30, 2005 (v1.0).

<sup>4</sup>FERC Smart Grid Policy Statement, July 16, 2009.

<sup>5</sup>SGIPGB and SGIP Charter, *Version 1.2*, June 10, 2010; SGIP brochure created for the 2010 IEEE/PES Transmission & Distribution Conference & Exposition; [www.sgipweb.org](http://www.sgipweb.org).

ess for stakeholders to participate in providing input and cooperating with NIST in the ongoing coordination, acceleration and harmonization of standards development for the Smart Grid. The SGIP also reviews use cases, identifies requirements and architectural reference models, coordinates and accelerates Smart Grid testing and certification, and proposes action plans for achieving these goals. The SGIP does not write standards, but serves as a forum to coordinate the development of standards and specifications by many standards development organizations.

Thus, the SGIP not only identifies and addresses standardization priorities, but also plays a leadership role in facilitating and developing an information architecture, a cyber security strategy and a framework for testing and certification. It focuses on analysis and coordination of effort in helping NIST fulfill its responsibilities under EISA. The NIST Roadmap is the starting point for this activity.

The structure depicted in Figure 2 enables the SGIP to accomplish its complex and urgent work. The SGIP membership is led by three core teams—NIST, Plenary Officers and a Governing Board—and it is fully supported by an administrator. The Governing Board that I now chair maintains a broad community based perspective by having a breadth of experience, knowledge and involvement. It also holds consensus as a core value, ensuring that all legitimate views and proposals are considered. Key responsibilities include approving and prioritizing work programs, facilitating dialogue with standards development organizations and arranging for necessary resources for the SGIP.

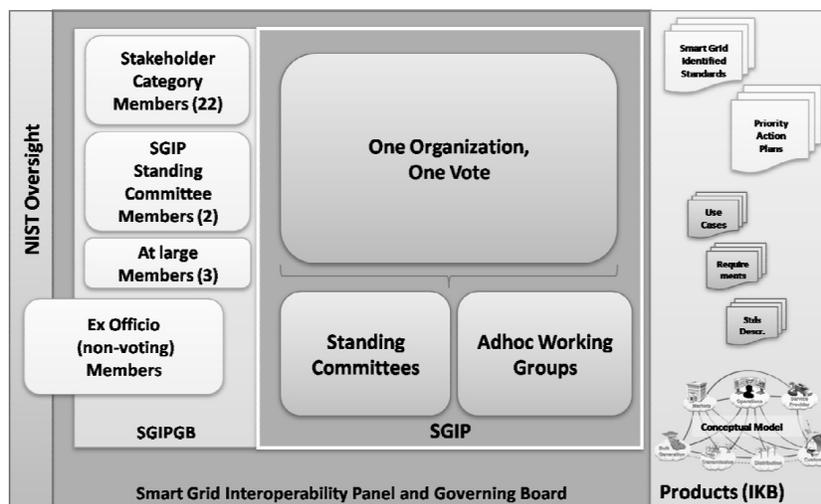


Figure 2 – The SGIP Structure

Our membership is large and diverse by design, as it is free and open to all who share the Smart Grid vision. To date, it consists of some 1,700 individuals from 590 member organizations (90% U.S., 5% Canada, 5% Other International) representing 22 stakeholder categories. Furthermore, the membership is organized into the following standing committees, working groups and teams, and is now supported by a Program Management Office.

- Standing Committees & Working Groups
  - Architecture (SGAC)
  - Cyber Security (CSWG)
  - Test & Certification (SGTCC)
- Domain Expert Working Groups
  - Transmission & Distribution (TnD)
  - Industry to Grid (I2G)
  - Building to Grid (B2G)

- Home to Grid (H2G)
- Vehicle to Grid (V2G)
- Business & Policy (BnP)
- Priority Action Plan (PAP) Teams
  - Meter Upgradeability Standard
  - Role of IP in the Smart Grid
  - Wireless Communications for the Smart Grid
  - Common Price Communication Model
  - Common Scheduling Mechanism
  - Standard Meter Data Profiles
  - Common Semantic Model for Meter Data Tables
  - Electric Storage Interconnection Guidelines
  - CIM for Distribution Grid Management
  - Standard DR and DER Signals
  - Standard Energy Usage Information
  - Common Object Models for Electric Transportation
  - IEC 61850 Objects/DNP3 Mapping
  - Time Synchronization, IEC 61850 Objects/IEEE C37.118 Harmonization
  - Transmission and Distribution Power Systems Model Mapping
  - Harmonize PLC Standards for Appliance Communications in the Home
  - Wind Plant Communications

### **SGIP Status Report**

To fully convey the effectiveness and progress of the SGIP to date, we need to address the following:

- What makes a standard? Why do standards not necessarily deliver interoperability? How can this be overcome?
- To what extent are currently available standards being implemented?
- How do we further advance the development of new standards?
- What ensures stakeholder buy-in and adoption of standards emerging from the SGIP process?
- How effective have we been in coordinating tasks and gathering stakeholder input in the SGIP process?
- What progress have our working groups and teams made since inception?

### *Relating Standards and Interoperability*

With respect to a technical standard, conformance, interoperability and performance are critical. Technology may be developed in accordance with the standard, and it may even fully perform in a formal stress test state of heightened activity. However, there remains room for interpretation in how the technology is implemented, how it ultimately operates in conjunction with other technology. This differential between compliance in design and ease of use in system operation speaks to the technology's interoperability.

As we strive for interoperability across Smart Grid's system of systems, we strive for compatibility, even interchangeability, which goes beyond the everyday talk of plug and play. Getting all the devices and infrastructure to speak a common language, use common interfaces and really work in unison is a new reality for both suppliers and customers that have traditionally operated in silos, built around specific functionality and/or areas of expertise. From the utility's perspective today, a supplier needs to ensure interoperability of technology not only within its own portfolio, but also with the technology portfolio from competing suppliers. This provides confidence in the technology investment and, ideally, a better return on the investment due to fewer, more easily managed implementations and/or integrations. The creation of the SGIP, with its knowledge and focus on all the building blocks of Smart Grid and the networked domains they reside in, reinforces the need and provides a forum for more coordinated and further structured implementation of standards.

### *Encouraging Implementation*

With all technical standards, we must also address the issue of application and use. The industry should be leveraging standards already developed and tested, even if the implementation of these standards needs to be further refined to promote interoperability. The major barriers to overcome in this area are awareness and risk aversion.

In the U.S.A., the transition from DNP 3.0 to IEC 61850 for substation automation and communications is an excellent example of the challenge we have before us. IEC 61850 calls for sending protection messages over Ethernet local area networks (vs. dedicated copper wires) and accessing measurements via a central process bus (vs. wired to the individual relays). These relatively small technology changes, but large process and cultural changes, have resulted in continued performance with substantial savings for those deploying this new technology worldwide. But there is enough concern and resistance to these changes here in the USA that IEC 61850 is not yet widely accepted or deployed.

Currently, standards development organizations and suppliers do little to educate utilities about standards, their features, benefits and overall value. The education required is comprehensive and constant in nature, to address awareness, trial/usage, acceptance and adoption, even recommendation. In addition, there is apprehension on the part of some utilities and regulators that needs to be addressed. Is the technology proven, at scale, in a real-life operating environment? Is it hardened to withstand changes in that environment? Does the technology adhere to standards? If so, which standards? And will those standards stand the test of time?

To address awareness and risk aversion, we need engagement, active participation and collaboration among a fully representative set of stakeholders. Being part of the process is paramount to trusting the process and its outcomes. The SGIP embodies and promotes these principles. The charter, membership profile and structure of the organization clearly demonstrate the desire to be open and inclusive in composition, transparent in operations and in consensus with work product and deliverables. The Governing Board is constantly evaluating balance among stakeholders, particularly, suppliers and utilities. This is required for the SGIP to drive standards that are technically strong and able to be successfully implemented—affordably and without adversely affecting performance.

### *Addressing the Speed of Standards Development*

The SGIP desires to create both a sense of stability and a sense of urgency with standards development. Suppliers may resist implementing technology that is not yet anchored to a standard. Utilities may also resist, and further require independent third party assurance of conformance once the technology is anchored to a standard. Timely development and implementation of standards are a priority, as delay may be a bigger risk for Smart Grid than balkanization. Our goal is to provide direction and a rapid path forward in that direction. To that end, the SGIP now has the ability to encourage standards development organizations to fast track a standard. This essentially means that NIST and the SGIP facilitate requirements capture, communicate a sense of urgency and push for expedited timetables with standards development organizations that still retain control of the actual development. The SGIP can also create additional PAPs as they are needed.

With respect to fast track, we should look to IEEE 1613, a standard for environmental requirements for networking equipment in the substation. The use of off the shelf retail networking equipment was a growing concern, creating an immediate need for hardened commercial equipment. The IEEE accomplished their task in just 18 months versus the usual four or more years and, this was back in 2003, well before the Smart Grid, NIST and the SGIP altered the landscape.

Additionally, when the SGIP—just three months in existence—recognized the growing importance of bringing and then managing wind on the grid, it quickly added PAP 16 around wind plant communications.

I also want to point out that, given the scope and pace of the SGIP agenda, we have recently established a Program Management Office to further coordinate and expedite the work of the various PAP teams. We have to ensure that we do not duplicate effort within the SGIP, and that technologies that are needed by multiple PAPs have consistency.

### *Achieving Stakeholder Buy-In and Adoption*

As NIST and the SGIP continue their efforts, we have every reason to believe that we have created the right environment for private sector buy-in and support of Smart Grid standards. In addition to policies and procedures around membership,

committee participation, work planning, project management, conflict resolution and the nomination and election of the SGIP leadership, we have influential parties including the DOE, FERC and the Office of Management and Budget (OMB), along with state regulatory and international agencies, who are shaping our initiatives.

The DOE funding announcements for the Smart Grid Investment Grant Program and Smart Grid Demonstration Program emphasize the importance of addressing interoperability and providing a summary of how a project will support compatibility with NIST's emerging Smart Grid standards framework and roadmap. As the grants are currently driving the majority of Smart Grid deployments, this tie to NIST and the work of the SGIP is important.

In addition, NIST expects that standards be produced and maintained by recognized standards development organizations as described in OMB Circular A-119 and the National Technology Transfer and Advancement Act. This ensures that standards and conformity assessment activities are acceptable for reference by Federal and state regulators. Some regulators further assert that the American National Standards Institute (ANSI) or an ANSI-accredited organization be involved so that there is greater assurance of openness and consensus. Given the regulatory construct for our largest investor owned utilities and the significant business they generate for suppliers, the private sector will buy-in and adopt what the public sector will authorize and approve.

#### *Guiding Development and Adoption Internationally*

For global suppliers like GE, working closely with any and all standards development organizations that have ANSI type processes and a culture of openness and consensus is essential for both speed of development and stakeholder buy-in. The adoption of open, international standards means that the technology investments we make and solutions we provide can be most cost effectively developed and produced to serve the largest possible population.

Thus, while NIST and the SGIP have influence with national organizations, they must continue to gain traction and favor with international organizations such as the International Electrotechnical Commission (IEC) and the Internet Engineering Task Force (IETF). Outreach to and involvement with the IEC and IETF are required for the NIST model of coordination and collaboration to be adopted rather than merely replicated region by region. Standards that become regionalized and fragmented create difficulties for suppliers and unnecessary risks for the future of Smart Grid.

#### *Ensuring Effectiveness of the SGIP Process*

In all of the areas previously discussed in this SGIP status report, it is evident that the SGIP has been effective in coordinating tasks and gathering stakeholder input. Since the beginning of the year, NIST and the SGIP have gained interest and traction worldwide on their Smart Grid Conceptual Reference Model. The identification and prioritization of the 75 existing standards of greatest impact to Smart Grid interoperability and the 16 Priority Action Plans to address gaps and inconsistencies are driving much needed focus, while the SGIP structure and operating rhythm are driving much needed collaboration and consensus. Timelines are being adhered to, even accelerated, in light of related policy discussions and actions. Meetings are being co-located with other stakeholders and industry influencers to further harmonize our respective work. Examples of this include Connectivity Week with IEEE in May and the National Association of Regulatory Utility Commissioners Summer Committee Meetings in July. Just as the Smart Grid is new, expansive and virtually all encompassing, so is the work of the SGIP. Yet, we are being nimble and reacting quickly to meet our goals, exceed industry expectations and encourage the international community and other regional standards organizations to join in our efforts.

#### *Reporting Progress Made by the SGIP*

The overall PAP process is shown in Figure 3. Supporting accomplishments and timelines for each PAP, as presented in the May 24th Governing Board meeting, follow.<sup>6</sup> We are fortunate to be moving forward on all fronts, made possible by the commitment and contributions of our valued members.

<sup>6</sup>SGIP Governing Board Meeting, May 24, 2010, presentation materials.

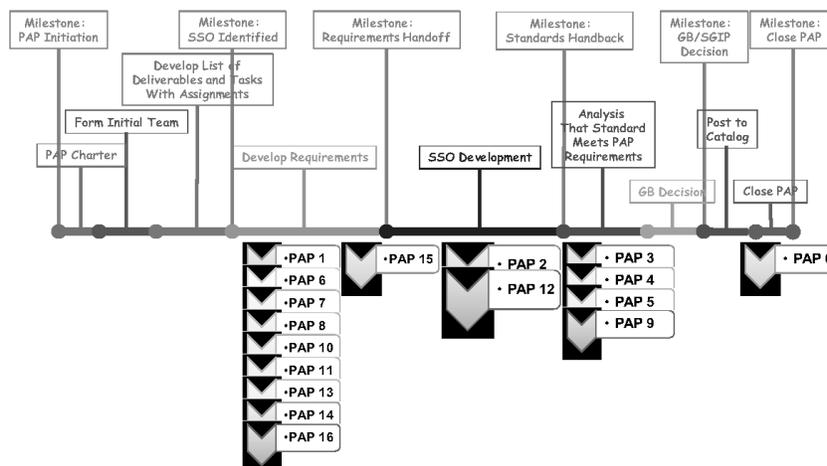


Figure 3 – PAP Process and Status

**PAP 0—Meter Upgradeability Standard:**

Complete. This effort resulted in the NEMA standard SG-AMI 1-2009 in September, 2009. The PAP was officially closed March 1, 2010.

**PAP 1—Role of IP in the Smart Grid:**

Quantified requirements for networking of Metering Systems and Initial Distribution Automation functions were completed.

**PAP 2—Wireless Communications for the Smart Grid:**

The wireless capability matrix for Smart Grid applications was completed. Final deliverables are expected in May and June, 2010.

**PAP 3—Common Price Communication Model:**

Use cases and requirements were completed. Combined PAP 3, 4, 9, 10 summit held in September, 2009. Draft specifications are in public comment period May 2010.

**PAP 4—Common Scheduling Mechanism:**

Standard XML serialization for bi-directional translation, use cases and requirements to test the standard, and web services Application Programming interfaces were completed. Combined PAP 3, 4, 9, 10 summit held in September, 2009. This PAP is expected to be closed in June, 2010.

**PAP 5—Standard Meter Data Profiles:**

AEIC guidelines with revisions were completed along with white paper descriptions and presentation materials. This effort is expected to be closed mid-summer, 2010.

**PAP 6—Common Semantic Model for Meter Data Tables:**

This PAP was dependent on PAP five and is now fully operational. Tasks and deliverables have been defined and use case analysis is currently underway.

**PAP 7—Electric Storage Interconnection Guidelines:**

A scoping study and key use cases and requirements were completed. These deliverables have directly affected an accelerated pace of activity on IEEE 1547 and IEC 61850-7-420 standards.

**PAP 8—CIM for Distribution Grid Management:**

Interoperability testing of CIM Wires Model and first set of key use cases and requirements are complete. Combined PAP 3, 4, 9, 10 summit held in September, 2009. Draft specifications are in public comment period May 2010.

**PAP 9—Standard DR and DER Signals:**

NAESB has collected, analyzed, and consolidate use cases and delivered requirements to PAP team.

**PAP 10—Standard Energy Usage Information:**

Contributions for supporting the requirements have been received from OpenADE, OpenHAN, EIS Alliance, and Zigbee. Requirements are being aggregated and a requirements review is imminent.

PAP 11—Interoperability Standards to Support Plug-in Electric Vehicles: Existing use cases and requirements identified and assembled. Coordination between SAE and IEC, alignment of vehicle information models, analysis of related standards, and connector alignment are ongoing.

PAP 12—IEC 61850 Objects/DNP3 Mapping: Use cases and requirements completed. Mapping is ongoing.

PAP 13—Time Synchronization, IEC 61850 Objects/IEEE C37.118 Harmonization: Harmonization use cases and requirements are complete. Gap analysis and mapping document are being completed in early summer, 2010.

PAP 14—Transmission and Distribution Power Systems Model Mapping: Developing use cases.

PAP 15—Harmonize PLC Standards for Appliance Communications in the Home: Completed requirements for wide band coexistence. Developing requirements for narrow band coexistence. IEEE and ITU modifying coexistence standards.

PAP 16—Wind Plant Communications: PAP approved. Charter completed. Team assembled. Tasks and deliverables identified. Use cases and requirements being developed.

As previously noted, the meter upgradeability standard (PAP 0) that gives guidance to utilities, regulators and others wanting to immediately deploy advanced metering infrastructure was completed last year. Other highlights since that May 24th Governing Board meeting follow:

- The team working on the development of energy usage information standards (PAP 10) recently reached a significant milestone. On June 23rd, the North American Energy Standards Board (NAESB) agreed to develop a basic energy usage data model standard, which the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) will extend for exchanging facility energy usage data with energy providers. NAESB has committed to complete the standard, which defines both the information used to communicate between utilities—and other sources—and the customer and how that information is organized, before the end of 2010.
- The team working on broadband and narrowband coexistence standards to provide for common communications mechanisms for appliance manufacturers (PAP 15) is nearing final selection of a supporting standards development organization.
- The SGIP just released a working draft of requirements for the essential application program interfaces for electronic calendars and schedules (PAP 4) and guidelines for “ANSI C12.19 End Device Communications and Supporting Enterprise Devices, Networks and Related Accessories” (PAP 5).

#### **GE Position on Standards**

Technical standards can accelerate innovation and investment in emerging technologies, provided those standards are developed and adopted in an open, consensus based fashion.

GE believes that the following principles should guide the Federal Government’s engagement in private sector standards activities:

1. Encourage consensus based adoption of technical standards
2. Balance Federal leadership with private sector innovation
3. Promote development of international standards
4. Utilize Federal R&D to support standards development
5. Educate stakeholders to accelerate deployment of standards

We shared these same principles with ANSI with respect to the recently announced National Science and Technology Council (NSTC) Subcommittee on Standards, and we would welcome further discussion if so desired.

#### **Concluding Remarks**

In closing, let me reiterate what Robert Gilligan, Vice President, GE Digital Energy shared in his testimony before the House Select Committee on Energy Inde-

pendence and Global Warming in February 2009. This is an unprecedented time in the energy industry. And, with respect to Smart Grid, this is definitely the time to be innovative, agile and willing to make bold moves. We are energized by the focus and momentum now surrounding Smart Grid and the solutions that enable energy efficiency, consumer empowerment and the integration of more renewable energy . . . solutions that in turn provide economic, environmental and energy security benefits to our nation.

We thank you, in advance, for your interest in and evaluation of how Smart Grid architecture and standards are progressing. As these represent the foundation we build upon, that will guide our technology development and innovation for years to come, it is essential we continue to move forward in a deliberate, disciplined fashion that represents and respects all industry stakeholders. While the work of NIST and the SGIP is extremely challenging, it is always rewarding given we are charting the course for a truly 21st century grid . . . steady, sustainable and truly smart.

Once again, we commend Chairman Wu for your leadership on these issues, and we appreciate the Committee's time and look forward to your questions.

#### BIOGRAPHY FOR JOHN D. McDONALD



John D. McDonald, P.E., is Director, Technical Strategy and Policy Development for GE Digital Energy. In his 36 years of experience in the electric utility industry, John has developed power application software for both Supervisory Control and Data Acquisition (SCADA)/Energy Management System (EMS) and SCADA/Distribution Management System (DMS) applications, developed distribution automation and load management systems, managed SCADA/EMS and SCADA/DMS projects, and assisted Intelligent Electronic Device (IED) suppliers in the automation of their IEDs.

John received his B.S.E.E. and M.S.E.E. (Power Engineering) degrees from Purdue University, and an M.B.A. (Finance) degree from the University of California-Berkeley. John is a member of Eta Kappa Nu (Electrical Engineering Honorary) and Tau Beta Pi (Engineering Honorary), is a Fellow of IEEE, and was awarded the IEEE Millennium Medal in 2000, the IEEE PES Excellence in Power Distribution Engineering Award in 2002, and the IEEE PES Substations Committee Distinguished Service Award in 2003.

In his twenty-three years of Working Group and Subcommittee leadership with the IEEE Power & Energy Society (PES) Substations Committee, John led seven Working Groups and Task Forces who published Standards/Tutorials in the areas of distribution SCADA, master/remote terminal unit (RTU) and RTU/IED communications protocols. John was elected to the Board of Governors of the IEEE-SA (Standards Association) for 2010–2011, focusing on long term IEEE Smart Grid standards strategy. John was elected to Chair the NIST Smart Grid Interoperability Panel (SGIP) Governing Board for 2010.

John is Past President of the IEEE PES, is a Member of IEC Technical Committee (TC) 57 Working Groups (WGs) 3 and 10, is the VP for Technical Activities for the U.S. National Committee (USNC) of CIGRE, and is the Past Chair of the IEEE PES Substations Committee. John was the IEEE PES Division VII Director in 2008–2009. John is a member of the Advisory Committee for the annual

DistribuTECH Conference, is a member of DOE's Smart Grid Electricity Advisory Committee (EAC), is a member of NEMA's Smart Grid Council, and is on the Board of Directors of the GridWise Alliance. John received the 2009 Outstanding Electrical and Computer Engineer Award from Purdue University.

John teaches a SCADA/EMS course at the Georgia Institute of Technology, a Smart Grid course for GE, and substation automation, distribution SCADA and communications courses for various IEEE PES local chapters as an IEEE PES Distinguished Lecturer. John has published thirty-four papers and articles in the areas of SCADA, SCADA/EMS, SCADA/DMS and communications, and is a registered Professional Engineer (Electrical) in California, Pennsylvania and Georgia.

John is co-author of the book Automating a Distribution Cooperative, from A to Z, published by the National Rural Electric Cooperative Association Cooperative Research Network (CRN) in 1999. John was Editor of the Substations Chapter, and a co-author, for the book The Electric Power Engineering Handbook, co-sponsored by the IEEE PES and published by the CRC Press in 2000. John is Editor-in-Chief, and Substation Integration and Automation Chapter author, for the book Electric Power Substations Engineering, Second Edition, published by Taylor & Francis/CRC Press in 2007.

Chairman WU. Thank you, Mr. McDonald.  
Mr. Eustis, please proceed.

**STATEMENT OF MR. CONRAD EUSTIS, DIRECTOR OF RETAIL TECHNOLOGY DEVELOPMENT, PORTLAND GENERAL ELECTRIC**

Mr. EUSTIS. Good morning Chairman Wu, Ranking Member Smith and other Members of the Subcommittee. My name is Conrad Eustis. I am the Director of Retail Technology Development of Portland General Electric. I have 35 years of experience in the power industry and 17 years implementing smart grid-related projects. Thank you for holding this important hearing on the development of standards for smart grid-related technologies.

Portland General Electric is Oregon's largest utility. We are an investor-owned utility serving approximately 820,000 customers in metro Portland and the Willamette Valley. We focus on providing reliable electricity at reasonable prices while continuing to be good stewards of Oregon's environment. PGE consistently ranks nationally near the top for renewable power sales customers. Long before the term "smart grid" arrived, PGE was implementing projects now labeled as smart grid. A few examples. We lead in our ability to operate our customers' standby generation during times of peak demand. We lead with innovative net metering programs to encourage solar development. We have had a residential time-of-use program available since 2001. And this August we will complete a systemwide installation of smart meters.

We are strong supporters of the NIST effort to achieve interoperability. I participate on NIST's Smart Grid Interoperability Panel and with other efforts. We feel that NIST leadership has implemented a number of useful policies to ensure industry buy-in; we highlight them in our testimony.

The NIST roadmap includes a testing phase to prove interoperability of selected standards among different manufacturers and devices. This is the most important part of the NIST plan and it is also the most important to ensure industry adoption. But it will probably be the most expensive and difficult. The testing process is also the best time to clarify, and prove, required cybersecurity methods.

Our written testimony elaborates on two suggestions to improve utility adoption of standards. We recommend efforts to understand, and then mitigate, the institutional barriers that our suppliers and our information technology departments face to adopt standards.

With regard to the availability of existing standards, it is important to understand that while there are many useful standards, interoperability requires multiple standards to achieve a specific end-to-end solution. While most systems purchased today implement one or more standards, interoperability still falls short because some standards are not developed. For example, where a communication device from one vendor is placed in the meter of another vendor, a meter data standard under ANSI [American National Standards Institute] helps reduce development time. However, because the physical method to pass data and the physical form factor have not been standardized, the integration of components still takes six to twelve months.

In establishing standards-related priorities, I think about criteria first. The first principle is that interoperability is most important when you talk about interconnecting low cost, mass-consumption products. For example, without interoperability, most home appliances can't be controlled economically. Second, standards adoption will likely be stronger by demonstrating an end-to-end solution that is visible to both customers and utilities. This means testing a set of standards to show an effective plug-and-play solution. Third, early successes will be more probable if we focus on very simple transactions. Additional, or more feature-rich modifications can be added to a standard later.

Guided by the principles above, I elaborate on three priorities in the written testimony. First, for home appliances, we need a standardized, USB-like socket together with a very simple transaction set to enable demand response programs. This is the lowest-hanging fruit on the smart grid tree and it would create interest for, and time for, consumers to learn about demand response. Second, we need a basic standard that allows electric vehicles to charge at the most opportune time. Electric vehicles represent a greenfield development process. They will have high visibility, and a standard will have wide adoption because it will not undergo undo an existing process. Finally, we need a standard for the format and process to send and receive usage data.

NIST is working on these last two suggestions but I want to reiterate that more than the standards themselves, testing them with a practical, end-to-end application is what will further adoption.

Thank you again, Chairman Wu, for your leadership and interest in this issue. I would be pleased to answer any questions the Committee may have.

[The prepared statement of Mr. Eustis follows:]

PREPARED STATEMENT OF CONRAD EUSTIS

Good morning Chairman Wu, Ranking Member Smith and other members of the subcommittee. My name is Conrad Eustis—I serve as Director of retail technology development at Portland General Electric. I have 35 years of experience in the energy business and 17 years of experience implementing successful smart grid related projects. In my role at PGE I participate on the utility's behalf in a number of regulatory and technical forums related to smart grid development, including the NIST standards process. Thank you for holding this important hearing on the development of standards for smart grid related technologies.

Portland General Electric is Oregon's largest electric utility. We are a vertically oriented investor-owned utility serving more than 817,000 customers in the Portland area and the Willamette Valley. We're focused on providing reliable electricity supplies at reasonable prices while continuing to be good stewards of Oregon's environment. In part, that means we're leading the charge on clean energy in Oregon.

I am sure it is no surprise to you, Mr. Chairman, that the U.S. Department of Energy has consistently ranked PGE as one of the top utilities for renewable power sales to residential customers. In fact, this year PGE earned DOE's top spot in the Nation for having more renewable power customers than any other utility in the nation.

We are also a recognized leader in the development of electric vehicle infrastructure. As a partner in the DOE's historic \$100 million ECotality grant, we expect to see more than 2,000 residential and public charging stations deployed in Oregon by 2013.

Long before the term "smart grid" became commonplace, PGE was investing in smart grid-related innovations—such as our Dispatchable Standby Generation (DSG) program in which we can remotely start and monitor our business customers' standby generation during times of peak demand. In exchange the utility installs telemetry equipment and contributes to its maintenance. We have worked with our regulators to support net metering for solar and other renewables. We've had a residential time-of-use program available since 2001. Today, we are actively deploying smart meters to all 817,000 customers throughout our service territory. We are 90 percent deployed and expect to complete deployment by the end of August. Ultimately, our goal is to be a leader in bringing the benefits of a smarter grid to our customers—providing them with more energy management options while increasing system reliability and efficiency.

Portland General Electric is also pleased to be a partner in the Pacific Northwest Smart Grid Demonstration Project, which will involve more than 60,000 metered customers in Idaho, Montana, Oregon, Washington and Wyoming. Using smart grid technologies, the study will test new combinations of devices, software and advanced analytical tools that enhance the power grid's reliability and performance.

As part of the study, PGE will implement a demonstration project on a distribution feeder in Salem serving residential and business customers. There are three primary objectives for this project: 1) to demonstrate how batteries together with demand response can be used to create a reliable micro-grid; 2) to determine how the batteries/inverter systems can be operated to provide peak-load following and frequency regulation; and 3) to determine how to position the batteries/storage to accept off-peak wind generation.

At the national level, we greatly appreciate the bipartisan support that passed the Energy Independence and Security Act (EISA) in 2007. That Act sets the course for the current standards making process at NIST and launched some of the most important policy changes for the utility sector in decades. With limited funding, NIST began implementing its responsibilities under EISA in 2008, establishing teams to collect stakeholder input, organizing meetings to create awareness of their effort to gain additional stakeholders and so forth. The passage of the American Recovery and Reinvestment Act provided the funds necessary to really launch this standards process and to create awareness across the 22 stakeholder groups that are required to implement a successful smart grid.

This effort is none too soon for the electric utility sector. Real challenges exist with the transition to lower carbon resources and the large-scale installation of intermittent renewable resources. This will force changes to system operation where smart grid transactions will be the most appropriate solution. However, I think many people have unrealistic expectations of how fast this change will come—even if a full set of standards were available today.

PGE learned that successful implementation of smart grid projects requires careful planning by a small team of cross-functional professionals working nearly full time for two or more years before launching the project implementation team. Successful implementation requires understanding the specific business processes that will need to change and identification of the legacy information systems that must be enhanced to support the new processes. Management must commit subject matter experts and provide training to support new departments while eliminating others. For most utilities, high public expectations for low-cost, reliable power means the vertical organization structure is lean and focused on existing processes. Since our industry has had, historically, levels of research and development expenditures below 0.2 percent of revenues, there are scarce funds and scarce resources available to staff the large project teams required to implement a smart grid project. This leads most utilities to seek regulatory support for a new smart grid project from their governance stakeholders. Regulatory buy-in involves more than just the regu-

lators. All, or at least most, stakeholders to the regulatory process must understand the value and benefits that smart grid will bring. This is not any easy task, and requires considerable time for education and due-diligence.

We are active participants in the NIST standards making process. I am PGE's participating member on NIST's Smart Grid Interoperability Panel, which had its first meeting in November of 2009. This panel includes 600 plus members from 22 stakeholder groups. To date, we have had only a small role coordinating tasks and gathering input. However, we serve a major role in keeping the more than 600 businesses we represent informed about the many parallel efforts taking place. The coordinating tasks have been managed by NIST directly or through the SGIPGB, and the Priority Action Plan team leaders.

One of the challenges with a standards making process is ensuring that you have industry support and a high level of adoption of the standards that eventually emerge from the process. We feel that NIST has implemented a number of policies to help ensure the utility industry buy-in. These include encouragement for all utilities to participate in the process, the recognition that there are multiple types of utility organizations, a fair governance process, and the beginnings of a public knowledge base to document support for implementing standards. NIST has also put together conferences that disseminate information, issue progress reports, and encourage face-to-face stakeholder input.

Looking ahead, NIST's plans for interoperability testing of standards will also be critical to ensuring industry adoption. Testing is critical with immature standards to determine where additional specifications are required to ensure interoperability. Because of the cost of testing, it also helps prioritize the initial requirements. It is not uncommon to overstate mandatory requirements to reach consensus in the definition stage; testing ensures the most important requirements are interoperable, and that different vendors interpret the written specification in the same way.

The NIST roadmap includes a testing phase to prove interoperability of selected standards from different manufacturers and devices. My understanding is that this phase has not started, or if it has, only recently so. This is the most important part of the NIST plan and will probably be the most expensive and difficult.

There are two additional activities that NIST could implement that we believe would likely improve utility buy-in and adoption.

The first has to do with the fact that the vendors—the suppliers of systems and equipment to utilities—enjoy a “seller's advantage.” For a given type of electric utility equipment there are usually about five major international suppliers. It is not uncommon for utilities to keep a relationship with one primary vendor and a second relationship with a back-up vendor. Part of the reason for this approach is because maintenance and operation of each vendor's equipment is somewhat unique to each vendor. While some aspects may be interoperable, the more complex features are often not. This is subtle example of non-inoperability and it allows vendors the opportunity to extract a larger profit margin because of a utility's reluctance to switch vendors. This is a gross simplification to make a point; there have been successes too—particularly in the area of interoperability for substation equipment. But the point remains that the higher margins created by partial interoperability is a potential barrier to higher levels of interoperability. NIST might consider as part of the early testing process, interviewing vendors separately and together to learn the needs of vendors to make standards adoption a higher priority.

Second, a focus on utility IT managers may be valuable. Among utilities, the responsibilities of VPs or general managers of the IT department vary greatly. For many of these managers, most of their time is spent keeping existing systems running smoothly; they have minimal time to focus on evolving and emerging standards. I would not be surprised to find that the average IT manager is minimally informed about the NIST process. NIST might consider engaging a diverse group of these managers, together with purchasing personnel that support them, to help keep them informed and to provide tools for them to require vendors to adopt specific standards. Some of the outcomes might be as easy as the publication of a quarterly update targeted to the utility IT manager.

NIST also needs to focus on developing standards and processes that make sense for consumers and addresses consumer behavior. For example, one complex and low priority transaction involves providing “real-time” time usage data from the meter to the home display. While desirable for some customers, most of the value in the usage data is available from non-real-time sources like a web page with perhaps a day of delay. PGE implemented a home display pilot in 2003. While half the customers found them interesting, most stopped accessing the displays after about a week. Energy is a low involvement product; effective smart grid implementations in the home will need to emphasize set and forget controls, and not depend entirely

on real-time involvement for their success. Spending time and money on programs consumers do not want should be avoided.

Now let me return to the issue of interoperability and its importance in the overall smart grid standards process. Fundamentally, the smart grid is about moving data from one system or device to another. This requires not one standard, but at least three to move one byte of data between two separate devices. If security is needed, this adds a fourth standard. In many systems purchased by utilities today, vendors focus on data transactions among devices in their product line. Generally, they design the transactions to minimize their cost to the customer utility—this is especially true of advanced metering infrastructure (AMI) systems. Where a communication device from one vendor is placed in the meter of another vendor, a meter data standard called ANSI C12.19 helps reduce development time. However, because the physical method to pass data and the physical form factor have not yet been standardized, the actual integration of the components still usually takes 6 to 12 months. For new two-way applications between the utility and the home, only immature standards exist. Between major utility enterprise systems—such as an outage management system—the use of a common information model at the application level is unfortunately rare. Small electric cooperatives, municipal utilities and PUDs that use a common application called MultiSpeak<sup>®</sup> are probably further along than the larger utilities who generally decide that custom applications serve their needs better.

The value in interoperability comes into play when you talk about the future for low-cost mass consumption products. Avoiding \$200,000 of custom engineering in a \$10 million substation because interoperability is available is still desirable, but the lack of interoperability doesn't prevent an economic implementation. But chasing after a peak demand savings of 50 watts in a common consumer item like a refrigerator would be impossible unless the total incremental cost is less than \$40. This cost can only be met via interoperability.

In thinking about what should be the top priorities for the NIST standards making process going forward, I believe the focus should be to create visible successes that can be implemented with end-to-end demonstrations. Early successes are possible if NIST focuses on very simple transactions; additional or more feature-rich modifications can be added to a standard later. These early successes will build upon themselves and create more utility interest and adherence to the NIST process. My top three suggestions along these lines are:

1) We need a standardized USB-like socket, together with a very simple transaction set, to enable demand response programs with home appliances. If appliance manufacturers were to incorporate these sockets on their major appliances over approximately five years, including the value-based appliances, utilities would gain the potential of 15,000 MW of demand response every year. Adding the socket without embedded communication hardware minimizes obsolescence and security issues. Since appliances last 10 to 30 years, making them demand response ready is important to prevent a lost opportunity in five to ten years as customer awareness increases. This is the lowest hanging fruit on the smart grid tree, and it would create interest for, and time for, customers to learn about demand response.

Some organizations advocate embedding a specific wireless<sup>1</sup> communication device in the appliance. While the free market should to some extent determine the best approach to creating "smart" appliances, security and interoperability are much more difficult to ensure with embedded communication devices. Consumer adoption of smart grid technologies could be threatened if even one or two bad experiences occur using embedded communication devices.

2) My second suggestion is for standardized smart charging for plug-in-vehicles (PIVs). This is not the same as the vehicle-to-grid concept, which will take more time and requires PIV manufacturers to gain more experience with the life of their batteries. This would be the basic standard for allowing PIVs to charge at the most opportune time. While the number of total PIVs in the near term will be small, the visibility of these vehicles as smart-grid friendly will be significant in the popular media. PIVs represent a "green field" development process and represent a great opportunity to gain wide adoption. This would counter the natural resistance that might occur from utilities and vendors to modify their existing systems to adopt a specific standard. Standards are easier to accept when you don't have to throw away something you already developed.

3) Finally, we need a standardized application for the format and process to send and receive usage data. This format would be used in multiple applications, for example: in meter-to-home applications, among back-office enterprise systems, utility-to-third parties, etc. In a year or two smart meters will be generating multiple

<sup>1</sup>Wireless includes radio and power-line communication techniques.

petabytes of usage data per year; we need a standard way to move meter usage information around.

Thank you, again, Chairman Wu for your leadership and interest in this issue. I would be pleased to answer any questions the committee may have.

#### BIOGRAPHY FOR CONRAD EUSTIS

Conrad Eustis has 35 years of experience in the energy industry including five years as a Naval officer in nuclear submarines, five years studying energy economics, technology and policy at Carnegie Mellon department's of Engineering and Public Policy, and 25 years at PGE leading new activities for the Company. He has technical degrees from both Carnegie-Mellon and Brown Universities.

The last 17 years of professional work have included the implementation of more than 20 "Smart Grid" projects in metering, demand response, home displays, smart appliances, web portals, utility enterprise systems development, and at least a dozen customer research projects. Conrad personally developed the design specifications for original hardware and software in many of these projects.

Career Highlights include:

- ◆ Engineer directing initial criticality on the refueled reactor of the USS Skate SSN 578 ('79)
- ◆ Ph.D. Thesis on policy to improve efficiency of cogeneration systems ('85)
- ◆ PGE's first demand—side resource plan; labeled as "innovate" by PUC ('90)
- ◆ Design and implementation of a critical peak pricing pilot (rate design and enabling hardware) '94
- ◆ Personal national award for an innovate electric vehicle infrastructure design ('95)
- ◆ Provided leadership for transactions to create interoperability in California's unregulated meter services market ('97)
- ◆ 10+ business cases for new smart grid platforms to deploy assets of > \$400 million, all reached executive approval for initial action steps, five reached operational status ('99 to '07)
- ◆ Provided technical and financial input to about ten fed-funded grant proposals leading to six successful awards ('93 to '09)
- ◆ Created Business Case, RFP, and Contract for current PGE smart meters project ('04 to '07)
- ◆ My influence helped earn PGE national awards for best smart meter implementation preparation ("Best Practices Award for Advanced Metering and Data Management", Chartwell, 2008), and meter data management leadership ("10 Years of Excellence Award", Metering America, 2009)
- ◆ Adjunct Professor at PSU teaching *Designing Smart Grid for Sustainable Communities*, '09 & '10
- ◆ Personal "Applied Award" for contributions to Interoperability from Gridwise Architecture Council ('10)

Chairman WU. Thank you, Mr. Eustis.

The votes have been called. There are about 10 minutes, 45 seconds left, and it is the intention of the Chair to proceed with Ms. Coney's testimony. Then I will ask one quick question and turn it over to Mr. Smith. We hope that he will get his questions in and then we will recess.

Ms. Coney, please proceed.

#### STATEMENT OF MS. LILLIE CONEY, ASSOCIATE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Ms. CONEY. Thank you. EPIC would like to thank the Subcommittee Chair and Ranking Member for this opportunity to speak with you on a matter that has emerged as one of the leading privacy challenges for our generation. Members of Congress, committees and their staffs from both sides of the aisle routinely approach EPIC on matters related to privacy and consumer rights.

Today, electricity usage generates 12 data points a year, the monthly bills that customers receive. The smart grid will raise that number to over 3,000 data points annually. As a result, the ability to assess consumer electricity usage information will pose significant privacy threats. These threats can include surveillance by government, businesses, and criminals.

Privacy is about the establishment and enforcement of fair information practices, or FIPs. The privacy impact assessment is an effective tool for evaluating whether fair information practices are enforced. The model many privacy advocates look to for real-world examples of what is possible to incorporate each of these components of privacy protection is the OECD Guidelines. The smart grid presents an extraordinary opportunity to establish a new approach where privacy is part of the architecture and R&D mindset of applications as they are developed. There can be security without privacy but there cannot be privacy without security. Smart grid customer data can pose physical dangers such as assaults, vandalism, home invasion, stalking, domestic abuse, targeting of homes for burglary or civil threats such as identity theft. Further, misuse of data by authorized parties such as data mining for resale or sharing of customer energy usage information or profiling of customers to further monetize their energy use presents privacy challenges to the smart grid adoption.

As EPIC looked to the participation in the standards process, we learned of the NIST smart grid recommendation drafting effort through two announcements published in the Federal Register on October 9, 2009. Later that month, we became aware of the working group effort to develop recommendations and sought out a NIST subject matter expert to get more information. EPIC encouraged the Electronic Frontier Foundation, the ACLU, the Privacy Rights Clearinghouse and others to join this effort. It is doubtful EPIC would have learned of the NIST effort on smart grid without the Federal Register notice process. The work on the NISTIR [NIST Interagency Report] on smart grid was far from smooth sailing, but overall it was productive and instructive for advocacy groups and utilities who value consumer privacy and potential partners from the online economy where consumer privacy is not as highly valued.

The NISTIR privacy subgroup for the project included those unfamiliar with privacy issues as well as privacy experts. The challenge was learning to speak the same language and understanding the core values of privacy as they relate to smart grid. The field of privacy is just like other disciplines: We learn from the mistakes and successes of others, improving our knowledge and understanding about what works and why. At present, the draft text incorporates a good statement on privacy and includes clearly supported language for fair information practices, recognizes the importance of privacy by design and other privacy-enhancing technology approaches, acknowledges the serious problem of reidentification first noted by Professor Latanya Sweeney at Carnegie Mellon University and by Professor Alessandro Acquisti at the same institution, and finally, details smart grid threats that include insecure smart meters, Internet access to smart grid data and third-party use of customer smart grid information.

However, as the document is merged with the remainder of the NIST Smart Grid Interoperability Standards Project, it will continue to be edited. The first draft will go to the Department of Commerce where it may further be edited prior to public release. The final document may bear little resemblance to the results of the privacy groups' hours of effort to address the unique privacy challenges of the smart grid. For this reason, EPIC reserves judgment on the success of including advocacy groups in the process until the final document is published.

Privacy protection is essential to the successful implementation of the smart grid and failure to develop robust standards that incorporate FIPS for protecting PII will likely hinder adoption of applications and services. Only by developing standards that ensure end-to-end privacy and security protection can NIST contribute to innovation and technology of the smart grid. NIST could fill an important role in establishing comprehensive privacy practices.

EPIC appreciates the Subcommittee's interest in smart grid privacy issues, is eager to contribute to the further development of smart grid privacy policy, and looks forward to the Committee's questions. Thank you.

[The prepared statement of Ms. Coney follows:]

#### PREPARED STATEMENT OF LILLIE CONEY

EPIC would like to thank the Subcommittee Chair and Ranking Member for this opportunity to speak with you on a matter that has emerged as one of the leading privacy challenges for our generation.

EPIC is a public interest research center, based in Washington, DC, established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values. EPIC has a long-standing interest and specialization in privacy and technology issues.<sup>1</sup> EPIC has a particular interest in the privacy implications of the Smart Grid standards, as we anticipate that this change in the energy infrastructure will have significant privacy implications for American consumers.<sup>2</sup> In other similar areas, EPIC has consistently urged Federal agencies to minimize the collection of personally identifiable information (PII) and to establish privacy obligations when PII is gathered.

It is rare today to discover an industry that collects, retains, and uses vast amounts of personal information that is also transparent, accountable, and operates collaboratively under state regulations. Utilities "do what they are told," adhering to rules established by public utility commissions and business models based upon fair information practices. The electric utility industry has done this for over one hundred years. It is EPIC's hope that they will adhere to this model of conduct as they move toward full deployment of the Smart Grid.

However, there will be great temptation to monetize the information about consumer electricity consumption in ways that may threaten consumer privacy, competitiveness of businesses, both small and large, and the security of Smart Grid infrastructure should it become a "plug and play" environment.

#### I. PRIVACY AND THE SMART GRID

##### A. DEFINING PRIVACY AND THE SMART GRID

Privacy is one of the most fundamental and basic of human rights. Without it, many other rights, such as the freedoms of speech, assembly, religion and the sanctity of the home, would be jeopardized. Although most countries around the world include explicit protection of a right to privacy in their constitutions, it remains one of the more difficult rights to define.

<sup>1</sup>EPIC, Electronic Privacy Information Center, <http://www.epic.org> (last visited June 29, 2010); EPIC, Privacy, <http://www.epic.org/privacy/default.html> (last visited June 29, 2010).

<sup>2</sup>EPIC, The Smart Grid and Privacy, <http://epic.org/privacy/smartgridsmartgrid.html> (last visited June 29, 2010).

The focus for protecting privacy of information stored on computers or exchanged on computing networks is determining whether data is or is not PII. This type of information can locate or identify a person, or it can be used in conjunction with other information to uniquely identify an individual. Historically, PII includes name, social security number, address, phone number, or date of birth. In the Internet Age, the list of PII has grown to include other data, including e-mail addresses, Internet Protocol (IP) addresses, social networking pages, search engine requests, log records, and passwords.

Our legal system has long recognized and protected an individual's right to personal privacy in PII. The drafters of the Constitution "conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized man. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation" of constitutional principles.<sup>3</sup> Moreover, public opinion polls consistently find strong support among Americans for legally cognizable privacy rights in law to protect their personal information from government and commercial entities.<sup>4</sup>

More recently, the Supreme Court, in *Kyllo v. United States*,<sup>5</sup> addressed the privacy implications of monitoring electrical use in the home. After reviewing precedent, the Court found that a search warrant must be obtained before the government may use new technology to monitor the use of devices that generate heat in the home:

[I]n the case of the search of the interior of homes—the prototypical and hence most commonly litigated area of protected privacy—there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that exists, and that is acknowledged to be reasonable. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment.<sup>6</sup>

The Court found that even the most minute details of a home are intimate: "[i]n the home, our cases show, all details are intimate details, because the entire area is held safe from prying government eyes."<sup>7</sup> Thus, the Court held that the police could not use thermal imaging equipment, which was not in general public use, "to explore details of the home that would previously have been unknowable without physical intrusion," without first obtaining a search warrants.<sup>8</sup>

#### B. ASSESSING SMART GRIDS AND PRIVACY

The Smart Grid implicates privacy at a fundamental level, as it can best be understood as a powerful digital communication network. Indeed, communications giant Cisco predicts the Smart Grid network will be "100 or 1,000 times larger than the Internet."<sup>9</sup> The Smart Grid would allow the unprecedented flow of information between power providers and power consumers. Its potential benefits to energy efficiency, granular control over power usage, and the environment are immense. However, like any analogous communications network, such as the Internet, the Smart Grid also admits the possibility of new and problematic threats to privacy in the form of increased data collection, retention, sharing and use.<sup>10</sup> As the National Institute of Standards and Technology (NIST) acknowledges, "[t]he major benefit provided by the Smart Grid, i.e. the ability to get richer data to and from customer meters and other electric devices, is also its Achilles' heel from a privacy viewpoint."<sup>11</sup>

<sup>3</sup> *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

<sup>4</sup> See generally EPIC, Public Opinion on Privacy, <http://epic.org/privacy/survey> (last visited June 29, 2010).

<sup>5</sup> 533 U.S. 27 (2001).

<sup>6</sup> *Id.* at 34.

<sup>7</sup> *Id.* at 37.

<sup>8</sup> *Id.* at 40.

<sup>9</sup> Martin LaMonica, *Cisco: Smart Grid Will Eclipse Size of Internet*, CNET, May 18, 2009, [http://news.cnet.com/8301-11128\\_3-10241102-54.html](http://news.cnet.com/8301-11128_3-10241102-54.html).

<sup>10</sup> See Ann Cavoukian, Jules Polonetsky & Christopher Wolf, Privacy by Design, *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation* 8 (Nov. 2009), <http://www.ipc.on.ca/images/Resourses/pbd-smartpriv-smartgrid.pdf> ("Modernization of the current electrical grid will involve end-user components and activities that will tend to increase the collection, use and disclosure of personal information by utility providers, as well as, perhaps, third parties.") [hereinafter Privacy by Design].

<sup>11</sup> National Institute for Standards and Technology, NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft) 84 (2009) [hereinafter Draft Framework].

The basic architecture of the Smart Grid presents several thorny privacy issues. The first widely distributed smart grid application is the smart meter.<sup>12</sup> Smart meters monitor and can report customer electricity consumption to the utility service provider. Experts estimate that U.S. investment in smart meters could total \$40 to \$50 billion, and that roughly one hundred million smart meters could be installed over the next five years.<sup>13</sup> Smart meters, like traditional meters, will be associated with a unique physical address, which makes it PII.<sup>14</sup> Along with the meter serial number and the electronic information associated with the meter address, this information is PII.

Smart meters will increase the frequency of communication from the home to the utility service provider or the third party application user. Traditional meter reading takes place once a month, by a visit from a person affiliated with the electricity service provider or billing company. In contrast, proposals for smart meters discuss “real-time” reporting of usage data.<sup>15</sup> Currently, the design specification is not for electricity consumption information to remain in the home or meter location, which could only be accessed easily by the utility user. Rather, the plan, as suggested in the Cyber Security Strategy, is to instead share the information with the utility company or others. If, as the document suggests, the information will allow customers to make better energy consumption decisions, then only the customer should have access to that information. This is one of many instances in which the design of a Smart Grid application can either favor privacy or ignore it.

Another architectural point which raises privacy implications is the use of wireless communications to transmit Smart Grid data.<sup>16</sup> The Draft Framework proposed to assess “the capabilities and weaknesses of specific wireless technologies.”<sup>17</sup> Although it mentions security as a characteristic of wireless technology that may be relevant to that assessment, privacy is not mentioned. Any wireless technology that would be used to transmit user data must protect personal privacy. Wireless sensors and networks are susceptible to security breaches unless properly secured,<sup>18</sup> and breaches of wireless technology could expose users’ personal data.<sup>19</sup> Similarly, the potential transmission of Smart Grid data through “broadband over power line” (BPL) implicates users’ privacy:

A BPL node could communicate with any device plugged into an electrical socket. Capture of a substation node would provide control over messages going to smart appliances or computing systems in homes and offices. A utility may also offer customers BPL as a separate revenue stream. This creates risks that [advanced meter] data could be read or modified over the internet or that common internet attacks could be brought against the electrical grid or individual customers.<sup>20</sup>

Moreover, wireless communication is especially problematic in light of how easily signals from wireless devices are detectable by bad actors to pick-up valuable information on systems using wireless technology, and the past exploitation of wireless

<sup>12</sup> See Stan Mark Kaplan, Congressional Research Service, *Electric Power Transmission: Background and Policy Issues* 23 (2009), available at <http://openers.com/document/R40511/2009-04-14/download/1013> (discussing basic functions of smart meters); U.S. Dep’t of Energy, *Smart Grid System Report* 38 (July 2009) [hereinafter “*Smart Grid System Report*”] (“The use of smart meters, a driving force behind being able to evaluate grid load and support pricing conditions, has been increasing significantly, almost tripling between 2006 and 2008 to 19 million meters . . .”).

<sup>13</sup> Draft Framework, *supra* note 11, at 21–22.

<sup>14</sup> See National Institute for Standards and Technology, Draft NISTIR 7628: Smart Grid Cyber Security Strategy and Requirements (2nd public draft) 33 (2010) [hereinafter Cyber Security Strategy], available at <http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628-2nd-public-draft.pdf> (flow chart detailing Smart Grid communication links between consumers and providers).

<sup>15</sup> See, e.g., Draft Framework, *supra* note 11, at 56.

<sup>16</sup> See Draft Framework, *supra* note 11, at 65.

<sup>17</sup> *Id.*

<sup>18</sup> See, e.g., Mark F. Foley, Data Privacy and Security Issues for Advanced Metering Systems (Part 2), [http://www.smartgridnews.com/artman/publish/industry/Data\\_Privacyand\\_Security\\_Issues\\_for\\_Advanced\\_Metering\\_Systems\\_Part\\_2.html](http://www.smartgridnews.com/artman/publish/industry/Data_Privacyand_Security_Issues_for_Advanced_Metering_Systems_Part_2.html) (“Wireless sensor networks, for example, are subject to the general security problems of computer networks, ordinary wireless networks, and ad-hoc networks”).

<sup>19</sup> See *id.* (breaches could “result in denial of service to customers or utilities (e.g., access to billing information or energy usage), payment avoidance, system overload, reduced quality of service, and violation of power control protocols”).

<sup>20</sup> *Id.*

systems by thieves who use techniques known as “wardriving” to seek out unprotected or insufficiently protected wireless communication portals.<sup>21</sup>

Wireless communications to transmitting Smart Grid data would not only provide a significant challenge to privacy of users, but may also pose economic and security threats. Identity theft, third party monitoring of utility use, home invasions, domestic abuse and predatory use of home electricity consumption information strips home owners of the protection from prying eyes provided by the walls of their home.

A final architectural problem with the proposed Smart Grid is the interaction between the Smart Grid and plug-in electric vehicles (PEV). It is possible that the Smart Grid would permit utility companies to use PEVs and other sources of stored energy “as a grid-integrated operational asset,”<sup>22</sup> *i.e.*, to drain the energy stored in the PEVs when the energy is needed to supply other users. This application of the Smart Grid is particularly troubling. If privacy is, as the Supreme Court has said, the “interest in independence in making certain kinds of important decisions,”<sup>23</sup> then this proposed application could severely damages both privacy interests and consumer rights.

### C. PRIVACY THREATS

In addition to the architectural weaknesses of the proposed Smart Grid, the application and use of the Smart Grid threatens privacy interests in many other ways.

#### i. MISUSE OF DATA

The massive amounts of data produced by the Smart Grid can potentially be misused by a number of parties—the power utilities themselves, authorized third parties such as marketing firms, or unauthorized third-parties such as identity thieves.

#### ii. POWER UTILITIES

Power utilities themselves will likely be interested in conducting complex data mining analysis of Smart Grid data in order to make power distribution decisions. For instance, at the Tennessee Valley Authority (TVA), administrators estimate that they will have 40 terabytes of data by the end of 2010, and that five years of data will amount to roughly half a petabyte.<sup>24</sup> The TVA administrators are actively working to improve their ability to analyze the data, including through “complex data mining techniques.”<sup>25</sup> Moreover, the TVA has explored using cloud computing resources to analyze and data mine the data, which raises a separate set of privacy concerns.<sup>26</sup>

#### iii. DATA MINING AND AUTHORIZED THIRD-PARTIES

Data mining of sensitive personal information raises serious privacy concerns.<sup>27</sup> For example, Total Information Awareness (TIA), developed by the Defense Advanced Research Projects Agency (DARPA), proposed to data mine wide swaths of information in order to detect terrorists.<sup>28</sup> However, privacy concerns led the Congress to eliminate funding for the project, and the Technology and Privacy Advisory Committee of the Department of Defense issued a report recommending that Congress pass laws to protect civil liberties when the government sifts through computer databases containing personal information.<sup>29</sup> The data mining of sensitive

<sup>21</sup> See, *e.g.*, Patrick S. Ryan, *War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics*, 9 VA. J.L. & TECH. 7 (2004).

<sup>22</sup> Draft Framework, *supra* note 11, at 67.

<sup>23</sup> *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977).

<sup>24</sup> Josh Patterson, Cloudera, *The Smart Grid and Big Data: Hadoop at the Tennessee Valley Authority* (TVA), June 2, 2009, <http://www.cloudera.com/blog/2009/06/02/smart-grid-big-data-hadoop-tennessee-valley-authority-tva>.

<sup>25</sup> *Id.*

<sup>26</sup> See EPIC, Cloud Computing, <http://epic.org/privacy/cloudcomputing> (last visited June 29, 2010).

<sup>27</sup> See EPIC, Terrorism (Total) Information Awareness, <http://epic.org/privacy/profiling/tia> (discussing government data mining of citizens’ personal information) (last visited June 29, 2010).

<sup>28</sup> See *id.*

<sup>29</sup> Department of Defense, *Safeguarding Privacy in the Fight Against Terrorism* (2004), available at <http://www.epic.org/privacy/profiling/tia/tapac-report.pdf>.

personal information transmitted through the Smart Grid raises similar privacy concerns.

Authorized third-parties may also be interested in using data collected through the Smart Grid. The real-time data streaming capabilities of the Smart Grid, in particular, implicate a separate group of privacy risks. Just as appliance manufacturers and insurance companies may want access to appliance usage data, marketing and advertising firms may want access to the data—particularly real-time data—in order to target marketing more precisely.<sup>30</sup> However, power usage data can reveal intimate behavioral information; providing that information to third-party marketing and advertising firms surreptitiously would be a repugnant invasion of privacy.

#### iv. IDENTITY THEFT AND DATA BREACHES

Further, without privacy standards that protect privacy there will be unauthorized third-parties who will likely also be interested in misusing Smart Grid data, for many of reasons such as identity theft or burglary. Identity theft victimizes millions of people each year.<sup>31</sup> The Federal Trade Commission (FTC) estimated that 8.3 million people discovered that they were victims of identity theft in 2005, with total reported losses exceeding \$15 billion.<sup>32</sup> According to the Privacy Rights Clearinghouse, more than 340 million records containing sensitive personal information have been involved in security breaches since January 2005.<sup>33</sup>

The faith placed in the capacity of the Smart Grid to safeguard sensitive personal information is unfounded. As an employee for Itron, a manufacturer of automated meters, admitted, “Any network can be hacked.”<sup>34</sup> Similarly, some experts argue that “an attacker with \$500 of equipment and materials and a background in electronics and software engineering could ‘take command and control of the [advanced meter infrastructure] allowing for the en masse manipulation of service to homes and businesses.’”<sup>35</sup> Thus, it is possible that “just as identities, credit and debit card numbers, and other financial information are routinely harvested and put up for sale on the Internet, so can Smart Grid identifiers and related information.”<sup>36</sup> Alternatively, identity thieves could use PII obtained elsewhere to impersonate utility customers, which poses the risk of fraudulent utility use and potential impact on credit reports.<sup>37</sup>

Peter Neumann, an expert on privacy and security who testified to the House Committee On Ways and Means Subcommittee On Social Security in 2007, concluded that the design of information systems are subject to many pitfalls, and that there is “[a] common tendency to place excessive faith in the infallibility of identification, authentication, and access controls to ensure security and privacy.”<sup>38</sup> As such, the dangers of identity theft and data breaches are a threat that must be addressed during the implementation of the Smart Grid.

<sup>30</sup> See *Privacy and the New Energy Infrastructure*, *supra* note 46, at 46; Rebecca Herold, SmartGrid Privacy Concerns, available at [http://www.privacyguidance.com/files/SmartGridPrivacyConcernsTableHeroldSept\\_2009.pdf](http://www.privacyguidance.com/files/SmartGridPrivacyConcernsTableHeroldSept_2009.pdf) [hereinafter Privacy Concerns]; Mark F. Foley, *The Dangers of Meter Data (Part 1)*, available at [http://www.smartgridnews.com/artman/publish/industry/The\\_Dangers\\_of\\_Meter\\_Data\\_Part\\_1.html](http://www.smartgridnews.com/artman/publish/industry/The_Dangers_of_Meter_Data_Part_1.html) [hereinafter “Dangers (Part I)”].

<sup>31</sup> See generally EPIC, Identity Theft, <http://epic.org/privacy/idtheft> (last visited June 29, 2010).

<sup>32</sup> Fed. Trade Comm’n, *2006 Identity Theft Survey Report* 4, 9 (2007) [hereinafter “FTC Survey Report”].

<sup>33</sup> Privacy Rights Clearinghouse, Chronology of Data Breaches, June 25, 2010, <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.

<sup>34</sup> Jeanne Meserve, ‘Smart Grid’ May Be Vulnerable To Hackers, CNN, March 21, 2009, <http://www.cnn.com/2009/TECH/03/20/smartgrid.vulnerability>.

<sup>35</sup> *Id.*

<sup>36</sup> Eric Breisach & H. Russell Frisby, *Energy Identity Theft: We’re Way Beyond Plugging in the Meter Upside Down*, Smartgridnews.com, April 9, 2008, [http://www.smartgridnews.com/artman/publish/article\\_425.html](http://www.smartgridnews.com/artman/publish/article_425.html).

<sup>37</sup> See Rebecca Herold, SmartGrid Privacy Concerns, available at [http://www.privacyguidance.com/files/SmartGridPrivacyConcernsTableHeroldSept\\_2009.pdf](http://www.privacyguidance.com/files/SmartGridPrivacyConcernsTableHeroldSept_2009.pdf) [hereinafter Privacy Concerns].

<sup>38</sup> *Security and Privacy in the Employment Eligibility Verification System (EEVS) and Related Systems: Hearing Before the H. Comm. On Ways and Means Subcomm. On Social Security*, 110th Cong. 9 (2007) (statement of Peter G. Neumann, Principal Scientist, Computer Science Lab, SRI International).

## v. UNAUTHORIZED ACCESS

The misuse of Smart Grid data is further exacerbated by the possibility of combining Smart Grid data with other data sources or scanning of open Home Area Networks that transmit Smart Grid energy usage data. For example, Google PowerMeter collects data on home energy consumption.<sup>39</sup> This technology raises the obvious possibility that Google will combine consumer information about power consumption with Google's preexisting ability to record, analyze, track and profile the activities of Internet users.<sup>40</sup> Such new business models also raise significant anti-trust concerns.<sup>41</sup>

The recent admission by Google that it secretly collected electronic PII from wireless networks around the world is particularly telling. For years, Google used its Street View data collection project to access and download data from unsecured wireless computer devices in homes and businesses without providing notice to or acquiring consent from government bodies or individuals.<sup>42</sup> Google's failure to provide notice was especially troubling because it precluded governments from enforcing local laws and protecting the security, welfare, and values of their own citizens. Google's massive misuse of emerging technology highlights the potentially devastating consequences of newly deployed technologies, and the need for effective oversight. In another example of the dangers presented by unanticipated negative effects of new technology, microwave ovens were first made available to consumers before their safety was comprehensively evaluated. The spectrum range of these appliances had a disruptive effect on heart pacemakers. However, contrary to many recently developed technologies, microwave technology was transparent and therefore accessible for independent review and study, so the problem was easily identified and quickly remedied.

Indeed, these risks remain if even residual data is stored on Smart Grid meters. If data on Smart Grid meters are not properly removed, residual data could reveal information regarding the activities of the previous users of the meter.<sup>43</sup> Thus, the Smart Grid should be designed to avoid the unnecessary retention of PII. Moreover, the prospect of remote access to Smart Grid data could lead to unauthorized access and misuse of the data. Many companies and government agencies provide employees and contractors with remote access to their networks through organization-issued computing devices. Remote access to Smart Grid customer information or utility usage data should be prohibited except for service provision and maintenance. The misuse of Smart Grid data could also harm consumers' reputations in many different ways. The collection and sharing of Smart Grid data could cause unwanted publicity and/or embarrassment. Moreover, public aggregated searches of Smart Grid data could reveal individual behaviors. Finally, the aforementioned data aggregation and data mining activity could permit publicized privacy invasions.

## vi. PERSONAL SURVEILLANCE

The Smart Grid could also reveal sensitive personal behavior patterns. The proposed Smart Grid will be able to coordinate power supply in real time, based on the power needs of users and the availability of power.<sup>44</sup> For instance, "[e]nergy use in buildings can be reduced if building-system operations are coordinated with the schedules of the occupants."<sup>45</sup> However, coordinating schedules in this manner poses serious privacy risks to consumers. Information about a power consumer's schedule can reveal intimate, personal details about their lives, such as their medical needs, interactions with others, and personal habits making "highly detailed information about activities carried on within the four walls of the home will soon be

<sup>39</sup> Google PowerMeter, <http://www.google.org/powermeter> (last visited June 29, 2010).

<sup>40</sup> See generally EPIC, Privacy? Proposed Google/DoubleClick Merger, <http://epic.org/privacy/ftc/google> (last visited June 29, 2010).

<sup>41</sup> Cf. Statement of Interest of the United States of America Regarding Proposed Class Settlement, *The Author's Guild, Inc., et al. v. Google, Inc.*, No. 05 Civ. 8136 (DC), at 16–26 (S.D.N.Y. Sept. 28, 2009) (Department of Justice arguing that the proposed settlement regarding Google Books "may be inconsistent with antitrust law"). See generally EPIC, Google Books Settlement and Privacy, <http://epic.org/privacy/googlebooks> (last visited June 29, 2010).

<sup>42</sup> EPIC, Google Street View and Privacy, <http://epic.org/privacy/streetview> (last visited June 29, 2010).

<sup>43</sup> See *Privacy Concerns*, *supra* note 37.

<sup>44</sup> Draft Framework, *supra* note 11, at 51.

<sup>45</sup> *Id.* at 52.

readily available for millions of households nationwide.”<sup>46</sup> “[R]esearch has delineated the differences in availability at home for various social types of electricity consumers including working adults, senior citizens, housewives and children of school age.”<sup>47</sup> Similarly, the data could reveal the type of activity that the consumer is engaging in, differentiating between, for example, housework and entertainment, or even a consumer’s lifestyle by revealing that a consumer has a serious medical condition and uses medical equipment every night, or that he lives alone and leaves the house vacant all day.<sup>48</sup>

#### vii. ENERGY USE SURVEILLANCE

Smart Grid meter data may also be able to track the use of specific appliances within users’ homes.<sup>49</sup> These “smart appliances” would be able to communicate with the Smart Grid, transmitting detailed energy-use information and responding dynamically to price fluctuations and power availability. A smart water heater, for example, could engage in “dynamic pricing” by using “a device that coordinates with a facility’s energy-management system to adjust temperature controls, within specified limits, based on energy prices.”<sup>50</sup>

As other devices become commercially available that are designed to send consumption data over the Smart Grid, the collection of personal data could increase. For example, the monitoring of electricity consumption may require the registration of items within a home for monitoring by the utility company or a third party service provider. Smart Grid enabled appliances such as washers, dryers, air conditioners, central heating systems, water heaters, stoves, refrigerator, freezers, swimming pools and Jacuzzis consume large amounts of electricity, and may be associated with a fixed address such as a home. Each of these items may have a unique product manufacturer designation (e.g. Whirlpool, General Electric, etc.), product serial number, and the purchase history of the item which would include the purchaser’s name. Monitoring the function and operation of these items would be physically associated with an address, which is PII for those occupying the residence.

Further, it can be anticipated that the Smart Grid could track even smaller electricity usage. Smart plugs or outlets might report in real-time when a lighting fixture, lamp, computer, television, gaming system, music device, or exercise machine is operating and the duration of use. One scholar forcefully argues that the ability to monitor electricity use at such a granular level poses a serious threat to privacy:

This, more than any other part of the smart meter story, parallels Shelley’s fable of Frankenstein: while researchers do not currently have the ability to identify every appliance event from within an individual’s electricity profile, the direction of the research as a whole and the surrounding context and motivations for such research point directly to developing more and more sophisticated tools for resolving the picture of home life that can be gleaned from an individual’s electricity profile. Before the switch is thrown and the information unleashed upon the world for whatever uses willed, it may be prudent to look into data protections lest the unforeseen consequences come back to haunt us.<sup>51</sup>

Indeed, the potential amount of personal information that could be gleaned from smart appliances is colossal:

For example, it is suggested that the following information could be gleaned with the introduction of end-user components . . . : Whether individuals tend to cook microwavable meals or meals on the stove; whether they have breakfast; the time at which individuals are at home; whether a house has an alarm system and how often it is activated; when occupants usually shower; when the TV and/or computer is on; whether appliances are in good condition; the number of gadgets in the home; if the home has a washer and dryer and how often they

<sup>46</sup> Elias Leake Quinn, *Privacy and the New Energy Infrastructure* 28 (2009), available at <http://ssrn.com/abstract=1370731> [hereinafter *Privacy and the New Energy Infrastructure*]; see *Privacy Concerns*, *supra* note 37.

<sup>47</sup> *Privacy and the New Energy Infrastructure* at 26–27; see A. Capasso et al., *Probabilistic Processing of Survey Collected Data in a Residential Load Area for Hourly Demand Profile Estimation*, 2 *Athens Power Tech* 866, 868 (1993).

<sup>48</sup> *Privacy and the New Energy Infrastructure*, *supra* note 46, at 27 (“differences in consumption vary with the type of activity, and profiles of energy uses that differentiate between activities can be constructed for things like leisure time, housework, cooking, personal hygiene”); see Capasso, *supra* note 47, at 869.

<sup>49</sup> See, e.g., *Privacy by Design*, *supra* note 10, at 8–9.

<sup>50</sup> *Smart Grid System Report*, *supra* note 12, at 34.

<sup>51</sup> *Privacy and the New Energy Infrastructure*, *supra* note 46, at 28.

are used; whether lights and appliances are used at odd hours, such as in the middle of the night; whether and how often exercise equipment such as a treadmill is used.<sup>52</sup>

Perhaps even more problematic, much of the personal information which could be gleaned from smart appliances would not otherwise be available to outsider observers: “With the whole of a person’s home activities laid to bare, [appliance-usage tracking] provides a better look into home activities than would peering through the blinds at that house.”<sup>53</sup>

Not only could that information be used to extract even more intimate information from the usage data, but that information could also be used in ways that impact the user in tangential areas of their lives.<sup>54</sup> For instance, appliance usage data could be transferred to appliance manufacturers to respond to warranty claims. Or, the data could be transferred to insurance companies that may want the information as part of an investigation into an insurance claim.<sup>55</sup> Landlords could track the energy use and behavior patterns of renters/leasees. The data could even be used to impinge on civil liberties by facilitating censorship or limitation of activities based on energy consumption patterns.<sup>56</sup> For instance, “meter data could reveal resident activities or uses that utility companies may then subsequently decide are inappropriate or should not be allowed.”<sup>57</sup> Or more generally, energy service providers in possession of consumer data may simply choose to use the data for marketing purposes or to sell it on the open market for a multitude of applications such as behavioral advertising.

The possibility that the appliances could interface with the Smart Grid through IP-based networks further exacerbates these privacy issues. The Draft Framework raises indirectly the privacy risk that would arise in an IP-based power network: “An analysis needs to be perforated for each set of Smart Grid requirements to determine whether IP is appropriate and whether cyber security can be assured.”<sup>58</sup> The effect of IP-based networks on privacy must be part of that analysis, as IPv6 and the “Internet of Things” raise new privacy considerations. For instance, the IP addresses associated with appliances or other devices “could be used to track activities of a device (and an associated individual),” thereby revealing an individual’s health condition, daily activities, and other sensitive and private information.<sup>59</sup>

Moreover, allowing the devices access to the Internet will make them more vulnerable, increasing the likelihood of security breaches and loss of personal privacy: “All of these [Smart Grid] communication links introduce vulnerabilities, especially if they can be accessed over the Internet.”<sup>60</sup> The invasiveness of extracting appliance usage data from Smart Grid data, particularly from IP-enabled appliances, cannot be overstated as IP addressing in an IPv6 environment will make possible the unique identification of every single device in the home that receives electric power. This combined with collected creates a bundle of vulnerable PII.

#### viii. PHYSICAL DANGERS

Data collected by the Smart Grid could be used by criminals, such as burglars or vandals, to monitor real-time data in order to determine when the house is vacant.<sup>61</sup> As one Carnegie Mellon University researcher argued, “[w]e should not build a power system in which a hacker working for a burglar can tell when you are home by monitoring your control systems . . . .”<sup>62</sup>

<sup>52</sup> *Privacy by Design*, *supra* note 10, at 11.

<sup>53</sup> *Id.* at 25.

<sup>54</sup> See *Privacy Concerns*, *supra* note 37; *Dangers (Part I)*, *supra* note 30.

<sup>55</sup> See *Dangers (Part I)*, *supra* note 30.

<sup>56</sup> See *Privacy Concerns*, *supra* note 37.

<sup>57</sup> *Id.*

<sup>58</sup> *Draft Framework*, *supra* note 11, at 29.

<sup>59</sup> SANS Institute, *The Next Internet Privacy in Internet Protocol 5* (2004); see Commission To the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Internet of Things—An Action Plan for Europe 5–6* (2009) (“Social acceptance of [Internet of Things] will be strongly intertwined with respect for privacy and the protection of personal data, two fundamental rights of the EU.”).

<sup>60</sup> See M. Granger Morgan, et al., Carnegie Mellon University Department of Engineering and Public Policy, *The Many Meanings of “Smart Grid” 5* (2009), available at [http://www.epp.cmu.edu/Publications/Policy\\_Brief\\_Smart\\_Grid\\_July\\_09.pdf](http://www.epp.cmu.edu/Publications/Policy_Brief_Smart_Grid_July_09.pdf).

<sup>61</sup> See *Privacy and the New Energy Infrastructure*, *supra* note 46, at 30; *Privacy Concerns*, *supra* note 37; *Dangers (Part I)*, *supra* note 30.

<sup>62</sup> Morgan, et al., *supra* note 60, at 5.

Similarly, the Smart Grid affects the interaction between privacy and domestic violence/stalkers.<sup>63</sup> Stalking, domestic violence and intimate partner abuse are also the targets of evolving state and Federal policy.<sup>64</sup> Over the years this area has grown to include the protection of the privacy of stalking and domestic violence survivors.<sup>65</sup> As EPIC has repeatedly argued, domestic violence victims often have urgent needs for privacy, as they may need to keep personal data from their abusers. This type of abuse can also involve privacy violations such as surveillance, monitoring, or other stalking methods. For a domestic violence victim, the need for privacy is a need for physical safety. However, the Smart Grid could provide abusers with another method for tracking and monitoring their victims. For instance, an abuser could track a victim's daily activities in order to exercise greater control over her ability to contact the authorities or other aid. Similarly, the capabilities of the Smart Grid could affect even emancipated domestic abuse victims, as their former abusers may be able to relocate the victims using personal information transmitted through the Smart Grid.

## II. RECOMMENDED PRIVACY STANDARDS

### A. ADOPT FAIR INFORMATION PRACTICES

PII activity should, as mentioned, be limited to a permitted and specified purpose. EPIC agrees that "only the minimum amount of data necessary for the utility companies to use for energy management and billing should be collected."<sup>66</sup> EPIC also agrees that treatment of information must conform to fair information practices. However, NIST should specify that those practices match the practices identified in the HEW Report<sup>67</sup> and the OECD Privacy Guidelines.<sup>68</sup> As discussed, the HEW Report established fair information practices, based on five principles:

- (1) There must be no personal data record-keeping systems whose very existence is secret. (2) There must be a way for a person to find out what information about the person is in a record and how it is used. (3) There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent. (4) There must be a way for a person to correct or amend a record of identifiable information about the person. (5) Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.<sup>69</sup>

Similarly, the OECD Privacy Guidelines established eight principles for data protection that are widely used as the benchmark for assessing privacy policies and legislation: Collection Limitation; Data Quality; Purpose Specification; Use Limitation; Security Safeguards; Openness; Individual Participation; and Accountability.<sup>70</sup> The treatment of Smart Grid information should conform to those practices in the following manner:

<sup>63</sup> See generally EPIC, Domestic Violence and Privacy, <http://epic.org/privacy/dv> (last visited June 29, 2010).

<sup>64</sup> See, e.g., Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, 119 Stat. 2960 (2005).

<sup>65</sup> See EPIC, Violence Against Women Act and Privacy, <http://epic.org/privacy/div/vawa.html> (last visited June 29, 2010).

<sup>66</sup> *Id.* at 12.

<sup>67</sup> Dept. of Health, Educ. and Welfare, *Secretary's Advisory Comm. on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens* (Government Printing Office 1973) [hereinafter "*HEW Report*"].

<sup>68</sup> OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), [http://www.oecd.org/document/18/0,3343,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html) [hereinafter OECD Privacy Guidelines], reprinted in *The Privacy Law Sourcebook* 395-423 (Marc Rotenberg ed., 2004).

<sup>69</sup> *HEW Report*, *supra* note 67, at xx-xxiii.

<sup>70</sup> OECD Privacy Guidelines, *supra* note 68.

OECD Privacy Principle	Corresponding Smart Grid Principle
<u>Collection Limitation:</u> There should be limits to the collection of personal data; any such data collected should be obtained by lawful means and with the consent of the data subject, where appropriate.	Smart Grid service providers should limit collection of consumers' personal data; any such data collected should be obtained by lawful means and with the consent of the consumer, where appropriate. <sup>71</sup>
<u>Data Quality:</u> Collected data should be relevant to a specific purpose, and be accurate, complete, and up-to-date.	Data collected by Smart Grid service providers should be relevant to a specific purpose, and be accurate, complete, and up-to-date.
<u>Purpose Specification:</u> The purpose for collecting data should be settled at the outset.	The purpose for collecting Smart Grid data should be settled at the outset.
<u>Use Limitation:</u> The use of personal data ought be limited to specified purposes, and data acquired for one purpose ought not be used for others.	The use of Smart Grid personal data ought be limited to specified purposes, and data acquired for one purpose ought not be used for others.
<u>Security Safeguards:</u> Data must be collected and stored in a way reasonably calculated to prevent its loss, theft, or modification.	Smart Grid data must be collected and stored in a way reasonably calculated to prevent its loss, theft, or modification.
<u>Openness:</u> There should be a general position of transparency with respect to the practices of handling data.	There should be a general position of transparency with respect to the practices of handling Smart Grid data.
<u>Individual Participation:</u> Individuals should have the right to access, confirm, and demand correction of their personal data.	Smart Grid consumers should have the right to access, confirm, and demand correction of their personal data.
<u>Accountability:</u> Those in charge of handling data should be responsible for complying with the principles of the privacy guidelines.	Those in charge of handling Smart Grid data should be responsible for complying with the principles of the privacy guidelines.

Moreover, NIST should require enforcement of the guidelines in accordance with the *HEW Report*.<sup>72</sup> NIST should recommend enforcement mechanisms, such as civil and criminal penalties, injunctions and private rights of action. By specifying the parameters and enforcement of the fair information practices, NIST can require actual conformance, rather than loosely requiring treatment to "conform."

Several of the principles proposed by NIST reflect the FIPs contained in the *HEW Report* and the OECD Privacy Guidelines, which is commendable. However, the NIST guidelines also propose other principles that could be strengthened or improved upon.

#### B. ESTABLISH INDEPENDENT PRIVACY OVERSIGHT

The Cyber Security Strategy proposes that "[a]n organization should formally appoint personnel to ensure that information security and privacy policies and practices exist and are followed. Documented requirements for regular training and ongoing awareness activities should exist and be followed. Audit functions should be present to monitor all data accesses and modifications."<sup>73</sup>

It is essential to ensure that information security and privacy policies and practices exist and are followed. NIST proposes that "[d]ocumented requirements for regular privacy training and ongoing awareness activities for all utilities, vendors and other entities with management responsibilities throughout the Smart Grid should be created implemented, and compliance enforced." However, it may be insufficient

<sup>71</sup> "Consent" is widely understood as "any freely given specific and informed indication of a data subject's wishes by which the data subject signifies his agreement to personal data relating to him being processed." European Union Data Protection Directive, reprinted in *The Privacy Law Sourcebook* 450 (Marc Rotenberg ed., 2004).

<sup>72</sup> *HEW Report*, *supra* note 67, at xxiii.

<sup>73</sup> *Cyber Security Strategy*, *supra* note 14, at 9.

for organizations to simply provide privacy training to their employees or even to appoint dedicated privacy officers with audit functions.

For example, in an analogous situation, despite the training and audit authority conferred to the Chief Privacy Office of the Department of Homeland Security, that office has proven to be impotent, powerless to effectively protect privacy. On a range of issues, from whole body imaging to suspicionless electronic border searches, the Chief Privacy Officer for DHS has failed to fulfill her statutory obligations.<sup>74</sup> Accordingly, EPIC and other privacy and civil liberties groups have called for Congress to consider the establishment of alternative oversight mechanisms, including the creation of an independent office.<sup>75</sup> Without such an independent office,<sup>76</sup> it would be impossible to ensure the proper protection of privacy rights, because the decisions of the Chief Privacy Officer would continue to be subject to the oversight of the Secretary and the rest of the Executive branch.

Similarly, for Smart Grid organizations to appoint privacy personnel or simply train existing personnel would be an ineffective solution that would only serve to preclude the possibility of creating an independent position with actual authority to protect privacy. The better solution is simple—NIST should recommend that an independent Privacy Office, with completely independent authority be established, with power over all entities associated with the Smart Grid.

### C. ABANDON THE NOTICE AND CONSENT MODEL

The NIST principles rely heavily on the notice and consent model:

A clearly-specified notice should exist and be shared in advance of the collection, use, retention, and sharing of PII. Data subjects should be told this information at or before the time of collection . . . . The organization should describe the choices available to individuals and obtain explicit consent if possible, or implied consent when this is not feasible, with respect to the collection, use, and disclosure of their PII.<sup>77</sup>

As a threshold matter, the purposes for which PII can be collected, used, retained, or shared should be severely restricted. The purposes for which PII can be collected, used, retained, or shared should be severely restricted. It is insufficient to simply require authorities or organizations to have a nebulous “purpose,” as anything from “improved marketing” to “government surveillance” could qualify. NIST should recommend that a formal rulemaking be established so that service providers establish a concrete set of approved purposes for which PII activity is permitted. That list of approved purposes should be very limited, and only purposes essential to the functioning of the Smart Grid should be permitted.

Once permissible purposes are established, data subjects should always be informed of the purpose of any collection, use, retention, or sharing of any PII. However, the “notice and consent” model is fundamentally flawed and should not be relied upon to excuse or justify any PII activity. As David Vladeck, Director of the Bureau of Consumer Protection at the Federal Trade Commission, recently acknowledged, the model simply does not function as intended:

[The notice and consent model] may have made sense in the past where it was clear to consumers what they were consenting to, that consent was timely, and where there would be a single use or a clear use of the data. That’s not the case today. Disclosures are now as long as treatises, they are written by lawyers—trained in detail and precision, not clarity—so they even sound like treatises, and like some treatises, they are difficult to comprehend, if they are read at all. It is not clear that consent today actually reflects a conscious choice by consumers.<sup>78</sup>

<sup>74</sup> See EPIC, Department of Homeland Security Chief Privacy Office and Privacy, <http://epic.org/privacy/dhs-cpo.html> (last visited June 29, 2010).

<sup>75</sup> Letter from EPIC, et al., to Representatives Bennie G. Thompson and Peter T. King (Oct. 23, 2009), available at <http://epic.org/security/DHS-CPO-Priv-Coal-Letter.pdf>.

<sup>76</sup> See, e.g., European Commission, Data Protection—National Commissioners, [http://ec.europa.eu/justice\\_home/fsj/privacy/nationalcomm/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm) (last visited June 29, 2010); Office of the Privacy Commissioner of Canada, [http://www.priv.gc.ca/index\\_e.cfm](http://www.priv.gc.ca/index_e.cfm) (last visited June 29, 2010); Office of the Privacy Commissioner for Personal Data, Hong Kong, <http://www.pcpd.org.hk> (last visited June 29, 2010).

<sup>77</sup> Cyber Security Strategy, *supra* note 14, at 105.

<sup>78</sup> David Vladeck, *Privacy: Where do we go from here?*, Speech to the International Conference of Data Protection and Privacy Commissioners, Nov. 6, 2009, available at <http://www.ftc.gov/speeches/vladeck/091106dataprotection.pdf>.

Indeed, in EPIC's testimony before the United States Senate Committee on Commerce, Science and Transportation, Marc Rotenberg argued that "[s]olutions which rely on simple notice and consent will not adequately protect users."<sup>79</sup> In an analogous context—notice and consent in online agreements—the failures of the model become more obvious. A recent survey of California consumers showed that they fundamentally misunderstand their online privacy rights.<sup>80</sup> In two separate surveys almost 60% of consumers incorrectly believed that the presence of “privacy policy” meant that their privacy was protected.<sup>81</sup> In a different survey, 55% of participants incorrectly believed that the presence of a privacy policy meant that websites could not sell their address and purchase information.

Users also routinely click through notices. The Pew Internet and American Life Project found that 73% of users do not always read agreements, privacy statements or other disclaimers before downloading or installing programs.<sup>82</sup> In such an environment, merely giving notice to users before collecting their sensitive information fails to adequately protect privacy in the way consumers expect.

Consumer data should instead receive substantive and ongoing protection. Especially because of the pervasiveness of the proposed nation-wide Smart Grid, choice and consent of individuals' is severely restricted. In all likelihood, individuals who wish to receive electricity will have little or no choice but to comply with policies that require the disclosure of PII. For authorities or organizations to obtain the consent of individuals would be nearly meaningless, as the power dynamic is fatally skewed. Information should be kept securely, and users should have the ability to know what data about them is being kept, to understand with whom it has been shared and to withdraw consent for the holding of this data. Further, data should only be collected and kept for specified purposes. Authorities and organizations must limit the collection, use, retention and sharing of PII in the first instance, rather than relying on hollow consents to justify more data collecting activity.

#### D. IMPOSE MANDATORY RESTRICTIONS ON USE AND RETENTION OF DATA

NIST must ensure that restrictions on the use and retention of data is mandatory, not aspirational. The NIST guidelines propose that: “Information should only be used or disclosed for the purpose for which it was collected, and should only be divulged to those parties authorized to receive it . . . PII should only be kept as long as is necessary to fulfill the purposes for which it was collected.”<sup>83</sup>

It is insufficient to simply say that information *should* be used or disclosed only for a permitted purpose. Instead, NIST must *require* organizations to follow those policies, and must provide the authorities with the power to enforce them.

Furthermore, it is inadequate to permit PII to be retained “as long as is necessary to fulfill the purposes for which it was collected.” That standard is entirely too lenient, and it would permit organizations too much leeway to retain information whenever they deem it necessary. Instead, NIST should set expiration dates on PII so that PII can be retained only for a certain period of time.<sup>84</sup> The length of time could vary based on the type of PII and the purpose for which it was collected. A concrete expiration date would make the system more transparent for consumers, as they would be more aware of the lifespan of their data.

NIST should also implement role-based access control to Smart Grid data. NIST has done significant work on the topic of role-based access control to computer records and systems. In this context, role-based access control protocols should strictly manage when, where, who and how PII in Smart Grid data is accessed. Access to PII, including electricity usage, should be limited to the function of the position an individual fills within the Smart Grid service delivery and billing relationship. Graduated levels of access should be based on responsibilities for providing Smart Grid FIPs and service provision purposes. Access should be monitored by log

<sup>79</sup> *Impact and Policy Implications of Spyware on Consumers and Businesses: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 110th Cong. (2008) (statement of Marc Rotenberg, President, EPIC).

<sup>80</sup> Joseph Turow, et al., *Consumers Fundamentally Misunderstand the Online Advertising Marketplace* (Oct. 2007), available at <http://groups.ischool.berkeley.edu/samuelsclinic/files/annenbergsamuelsadvertising.pdf>.

<sup>81</sup> *Id.* at 1.

<sup>82</sup> Pew Internet & American Life Project, *Spyware: The Threat of Unwanted Software Programs is Changing the way People use the Internet*, 6 (July 2005), available at [http://pewinternet.org/pdfs/PIP\\_Spyware\\_Report\\_July\\_05.pdf](http://pewinternet.org/pdfs/PIP_Spyware_Report_July_05.pdf).

<sup>83</sup> Cyber Security Strategy, *supra* note 14, at 106.

<sup>84</sup> See Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (2009) (arguing that digital information should have expiration dates, which will enable people to both control the sharing of information with others, as well as be more aware of the “finiteness of information”).

files and auditing of access use and resolution of issues related to customer service and proper operation of the Smart Grid.

Finally, NIST should explicitly address law enforcement access to Smart Grid data and should ensure that their access complies with the strictures of the Fourth Amendment. As discussed,<sup>85</sup> the Supreme Court in *Kyllo v. United States* addressed the interaction between the Fourth Amendment and the monitoring of electrical use, holding that the police could not use thermal imaging equipment not in general public use “to explore details of the home that would previously have been unknowable without physical intrusion,” without first obtaining a search warrant.<sup>86</sup> As the Court recognized, “At the very core’ of the Fourth Amendment ‘stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.’”<sup>87</sup> Similarly, in the Smart Grid context, NIST should make clear that the Fourth Amendment protects the information of Smart Grid consumers, and that law enforcement must first obtain a search warrant before gaining access to the information.

#### E. VERIFY TECHNIQUES FOR ANONYMIZATION OF DATA

The privacy risks associated with the use and retention of “anonymized data” are significant because such data may not be truly anonymous. Quasi-identifiers can be used for re-identification because they can be linked to external databases that contain identifying variables. This method, record linkage, occurs when two or more databases are joined. Such information can be obtained through public records, such as birth and death certificates.<sup>88</sup> Using record linkage, de-identified data can also be easily re-identified. For example, by utilizing date of birth, gender and zip code information for members of the public, a researcher was able to uniquely identify 87% of the U.S. population.<sup>89</sup>

Similarly, according to the GAO, complete SSNs may be reconstructed from truncated digits by simply comparing truncated SSNs in federally generated public records, which provide only the final four digits, to truncated SSNs provided by many information resellers, which provide only the first five digits.<sup>90</sup> Thus, by simply comparing the two records, a complete SSN can be reconstructed.<sup>91</sup>

Moreover, in a study published in July 2009, two researchers at Carnegie Mellon University found that an individual’s entire SSN often could be predicted from publicly available birth information.<sup>92</sup> The first five digits of an individual’s SSN could be predicted with a greater degree of accuracy. The accuracy of the researchers’ predictions was even greater when predicting the numbers of individuals born in sparsely-populated states like Montana, and the researchers anticipate that their predictions will become increasingly accurate over time. This research demonstrates the ineffectiveness of attempting to protect privacy by “anonymizing” or “de-identifying” data.

Techniques for anonymizing data should be pursued, but it is vitally important to ensure that such methods are robust, provable and transparent. Any technique proposed to anonymize data should be made public and available to researchers to examine and evaluate. Under no circumstance should a company be able to represent, without independent verification, that it had anonymized data. Until such techniques are established and safeguards are put in place, the primary objective should be to minimize the collection of PII in the first instance.

#### F. ESTABLISH ROBUST CRYPTOGRAPHIC STANDARDS

Strong cryptography should be applied to secure all electronic communications from a Smart Grid application or device. Threats to address include injection of false information; deletion of information, denial of service attacks, billing identity theft,

<sup>85</sup> See *supra* notes 5–8 and accompanying text.

<sup>86</sup> 533 U.S. 27, 40 (2001).

<sup>87</sup> *Id.* at 31 (quoting *Silverman v. United States*, 365 U.S. 505, 511 (1961)).

<sup>88</sup> See Salvador Ochoa et al., *Re-identification of Individuals in Chicago’s Homicide Database: A Technical and Legal Study*, Massachusetts Institute of Technology (2001) (utilizing the Social Security Death Index and de-identified information about Chicago homicide victims, the researchers were able to re-identify 35% of the victims).

<sup>89</sup> Latanya Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality*, 25 J. Law, MED., & ETHICS 98, 98–99 (1997).

<sup>90</sup> U.S. Gen. Accounting Office, *Identity Fraud Survey Report: Consumer Version 2–3* (2009).

<sup>91</sup> *Id.* at 3.

<sup>92</sup> See Alessandro Acquisti & Ralph Gross, *Predicting Social Security Numbers from Public Data*, 106 Proceedings of the National Academy of Sciences 10975.

service identity theft, malicious software, cyber attacks, pranks and various types of surveillance.<sup>93</sup>

The Billion-Dollar Bug Smart meters are extremely attractive targets for malicious hackers, largely because vulnerabilities can easily be monetized. Hackers who compromise a meter can immediately manipulate their energy costs or fabricate generated energy meter readings.

For this reason, there should be an open call for designs that seek to maximize both data security and privacy of the home as well as of enterprises. It is well known in the cryptographic community, for instance, that so-called “blind signatures” can allow ultra-secure reporting of energy usage statistics without revealing the precise appliance and timings involved.<sup>94</sup>

Sound cryptographic techniques do not rely upon hiding the cryptographic process, often referred to as an algorithm, from public review. Sound cryptographic processes are made so by the rigors imposed by public disclosure and testing of algorithms, and perhaps even more significantly, by the environment in which the cryptography is implemented.<sup>95</sup> Placing the strongest cryptography in an operating system or application that can easily be subverted by insiders, or compromised externally by penetration and malware can render the cryptography ineffective.<sup>96</sup> For this reason, it is imperative that all cryptographic algorithms used to secure Smart Grid technology and electronic technology used to facilitate Smart Grid optimization and operations be open for public inspection and testing and that the findings be made public, including the entire systems in which the cryptography is used. Further, encryption and decryption keys that are used to secure information stored or transmitted on the Smart Grid should be of sufficient complexity that they cannot be easily deduced or broken.

It is disconcerting that a document prepared by NIST on what will be the most significant leap forward in digital communication capability in thirty years had so little to say about cryptography. The document mentioned “cryptography” and “encryption” only twice, and both times were in a table on standards and applications.

### III. THE EFFECTIVENESS OF NIST-COORDINATED STANDARDS PROCESS IN GATHERING AND INCORPORATING THE INPUT FROM CONSUMER ADVOCACY ORGANIZATIONS

EPIC first became aware of the development of Smart Grid recommendations through two announcements published in the Federal Register on October 9, 2009. We later became aware of the working group effort to develop recommendations in mid-October 2009 and sought out a NIST subject matter expert to get more information on that effort. Tanya Brewer, with NIST Computer Security Division, and computer scientist Annabelle Lee were leading the effort on the NIST Smart Grid Interoperability Standards Project.

EPIC was made welcome to join the effort and I asked if it would be possible to include additional privacy organizations into the process. The response was that all would be welcome to participate in the privacy group. I coordinated the work of EPIC’s Privacy Coalition and invited members to participate in the effort. The Electronic Frontier Foundation, ACLU, and Privacy Rights Clearinghouse accepted the invitation. We joined the Future of Privacy Forum and the Samuelson Law Clinic at Berkley (which represented the Center for Digital Technology) in providing input on the privacy components to the Smart Grid document.

The meetings I attended with NIST staff were punctuated by an invitation to join the NIST Smart Grid Interoperability Standards Project drafting effort.

Whether EPIC would have known about the NIST Smart Grid Interoperability Standards Project without a vital link to our Advisory Board is doubtful. Consumer advocacy organizations and NIST do not normally travel in the same circles. A chance confluence of events made the participation in the NIST Smart Grid Interoperability Standards Project possible. The process was far from “smooth sailing,” but overall it was productive and instructive for groups that value consumer privacy and potential partners from the online economy, where consumer privacy is not as highly valued.<sup>97</sup>

<sup>93</sup> Patrick McDaniel & Stephen McLaughlin, Security and Privacy Challenges in the Smart Grid, IEEE SECURITY AND PRIVACY, May/June 2009, 75–77.

<sup>94</sup> David Chaum, Achieving Electronic Privacy, SCIENTIFIC AMERICA, Aug. 1992, at 96–101, available at [http://chaum.com/articles/Achieving\\_Electronic\\_Privacy.htm](http://chaum.com/articles/Achieving_Electronic_Privacy.htm).

<sup>95</sup> Bruce Schneier, *Applied Cryptography* 21–46 (2d ed. 1996).

<sup>96</sup> Peter Neumann, *Computer Related Risks* 132–180 (1995).

<sup>97</sup> EPIC, Social Networking Privacy, <http://epic.org/privacy/socialnet/> (last visited June 30, 2010).

The Privacy Group for the project included those unfamiliar with privacy issues as well as privacy experts. The challenge was learning to speak the same language and understanding the core values of privacy as they relate to Smart Grid. The field of privacy is just like other disciplines: we learn from the mistakes and successes of others, improving our knowledge and understanding about what works and why.

Critical to the Privacy Group's ability to work together was NIST's hosting two face-to-face meetings with participants. This helped to communicate the necessary breadth of privacy protection, which is neither a zero sum decision-making process nor a series of trade-offs. Rather, protecting privacy consists of a series of steps to assure that users retain the rights to control who, when, why, and how others may access information about themselves.

There were some rough spots as NIST computer security experts grappled with the language of privacy protection. There were discussions about whether Smart Grid data collection would introduce anything new about consumers or only make available information that was already public. There were discussions around common concepts like de-identification and re-identification, widely recognized terms within the field of privacy policy.

The conversations continued with a healthy exchange of ideas, until equilibrium was reached. The Privacy Group divided its work among legal, privacy, and technical experts to complete the draft of the privacy chapter. This is one of the most interesting aspects of the project; the people who worked on it were primarily volunteers, giving their time and talent freely.

The draft of the privacy chapter I received last week is a good document because it covers the basics of privacy and offers solid recommendations on how to address privacy in the Smart Grid. However, as the document is merged with the remainder of the NIST Smart Grid Interoperability Standards Project, it will continue to be edited. The final draft will go to the Department of Commerce, where it may further be edited prior to public release. The final document may bear little resemblance to the result of the Privacy Group's hours of effort to address the unique privacy challenges of the Smart Grid.

For this reason, EPIC will reserve judgment on the success of including advocacy groups in the process until the final document is published. To the degree that NIST remains free of politics and can remain rooted in science, it can serve the nation's best interest. The Smart Grid for some presents a grand opportunity to create energy independence for our nation, while for others it is an opportunity to open new markets and reap profits. Unfortunately, third-party energy management service providers may be more focused on the data they can access and monetize than the benefits to the consumer or energy independence.

#### IV. CONCLUSION

Privacy protection is essential to the successful implementation of the Smart Grid and failure to develop robust and implement privacy policy will hinder adoption of applications and services. Only by building privacy protection into the Smart Grid from the outset can the NIST defend the privacy interests long protected by our legal system. Thus, NIST should establish comprehensive privacy regulations that limit the collection and use of consumer data. EPIC appreciates the Subcommittee's interest in Smart Grid privacy issues, is eager to contribute the further development of Smart Grid privacy policy, and looks forward to the Subcommittee taking action in this area.

#### BIOGRAPHY FOR LILLIE CONEY

In 2009, House Speaker Nancy Pelosi appointed Ms. Lillie Coney to the Election Assistance Commission (EAC) Board of Advisors. Ms. Coney's work at EPIC encompasses original research and writing on topics that impact privacy rights and civic participation. In 2004, she contributed the chapter "Mobilize Underrepresented Voters," to the New York Times Bestseller, *50 Ways to Love Your Country*. In 2005, she co-authored, along with computing technologists and researchers, the paper, *Toward a Privacy Measurement Criterion for Voting Systems*. In 2006, Ms. Coney was the organizing force behind the first research conducted in a polling location to measure the usability of optical-scan and touch screen voting systems resulted in the report, *Voting Technology, Election Administration, and Voter Performance*, published by Stein, Vonnahme, Byrne, and Wallach (2008). In October 2008, EPIC's voting project published *E-Deceptive Campaign Practices Report: Internet Technology and Democracy 2.0*, the first report to review technology as a tool for online deceptive campaign practices. The report reviewed the potential for abuse of Internet technology in an election context, and made recommendations for steps that

could be taken by Election Protection, Election Administrators, and voters to protect the integrity of the upcoming election. In 2009, she coordinated and lead the audit review of the Punchscan Voting Systems use in the November 2009, Takoma Park Municipal election. She has written and spoken extensively on the subject of voting technology and privacy. She has published several law and policy journal articles on elections and voting systems.

Ms. Coney serves in an advisory capacity to Verified Voting, ACCURATE, Voting System Performance Rating, and Open Voting Consortium. She is also a member of the Association for Computing Machinery's Public Policy Committee.

Ms. Coney's work at EPIC includes coalition development and civil rights in the digital information age. She serves as the Coordinator for the Privacy Coalition, an EPIC project. The Privacy Coalition has over 40 organizations and affiliates, representing a broad political spectrum, committed to freedom and privacy rights. She manages monthly meetings of the Privacy Coalition as well as one annual conference held in January of each year. Guest speakers from previous administrations included: Chairs of the Federal Trade Commission, the Civil Liberties Protection Officer for the Office of National Intelligence, and the former Executive Director and Vice Chair of the Privacy & Civil Liberties Oversight Board. Ms. Coney has coordinated several major Internet Privacy advocacy campaigns; most notable are the "Stop REAL ID Campaign" and the "Stop Digital Strip Searches" efforts.

She has testified before the House Judiciary Committee on Privacy and Cybercrime Enforcement and the House Committee on Homeland Security on the topic of Watchlists. She also testified several times before the Department of Homeland Security's Data Privacy and Integrity Advisory Committee on domestic surveillance, CCTV Surveillance, and "Fusion Centers". Ms. Coney has testified before the Election Assistance Commission on the subject of voter registration database privacy, electronic voting system standards development, and developing reliable measures for voting administration and equipment management.

She also provides advice and input on privacy issues related to Cloud Computing and Smart Grid implementation.

Ms. Coney was the former Public Policy Coordinator for the Association of Computing Machinery (ACM). The ACM is the largest and oldest organization of computing professionals in the world. Prior to that, Ms. Coney served as special assistant to Rep. Sheila Jackson Lee (D-TX) on a variety of issues ranging from energy and information technology policy, election reform, to education policy. Her background includes extensive work in computer systems and technology policy. She has over 18 years of experience working on science and technology issues. She also has worked with civil rights and grassroots organizations on issues of voting and civil rights.

Ms. Coney received a B.A. in Political Science and a Masters in Public Administration from Lamar University in Beaumont, Texas. She is a former Systems Administrator who has designed and developed web sites for Congressional offices.

Chairman WU. Thank you very much, Ms. Coney, and thank you for your very, very interesting written testimony also.

I am going to ask one question to start and then turn it over to Mr. Smith. The utility business or the electric grid is dominated by very large players, by utilities. General Electric is not a small player. We have seen some of the research and development, particular technology development, benefits of having small high-tech startups, whether it is in the electronic hardware business or in software or in biotechnology. Think through for me, anyone who wants to address this, what the standard-setting process and what other things we can do to harness the small-business capacity and particularly the high-tech startup folks so that they can contribute as they have contributed with great success to other technologic development fields, anyone who wants to address that. Mr. Eustis.

Mr. EUSTIS. Yes. I work with a number of entrepreneurial groups back in Portland, and they do very much need standards as a way to get access, for example, to meter data as a way to implement energy management systems in the home versus right now it is a custom implementation with every utility. Standards are essential to creating innovation.

Chairman WU. A wider playing field for any startup.

Mr. EUSTIS. Yes, sir.

Chairman WU. Thank you very much.

Dr. Arnold?

Dr. ARNOLD. Well, we have certainly gotten a lot of startups and small companies involved in the Smart Grid Interoperability Panel, and one indicator of that is that we have about a dozen venture capital firms who are members of the panel and so clearly there is great interest in startups and innovation.

Chairman WU. Mr. McDonald.

Mr. McDONALD. One of the things with smart grid as shown by the reference model that NIST prepared was it is very expansive. It covers—the domain is from the generation plant all the way down to the home. We find no matter how big of a company, even GE, we need small startups. We need other companies to partner with us to be able to provide the technology for smart grid. So we formed a strategic partner organization. We are constantly talking with startups and new companies to fill the gaps that we don't provide ourselves, and in doing that we bring them in to the standards arena because standards is very important to us, and if the startup company that we are going to partner with doesn't embrace standards, we make sure that that happens and we work closely with them in that regard. Thank you.

Chairman WU. Thank you very much, Mr. McDonald. I just want to add that whether U.S. General Electric or Intel, IBM, Westinghouse, the example from other industries has been that when the startups are permitted to play, they frequently contribute to the ecosystem and further development of the field and occasionally there are acquisitions also that add to larger companies.

We have 327 not voted, and I think we can push it down another 100. Ms. Coney, you wanted—

Ms. CONEY. Yes, I wanted to add that the utility industry for over 100 years has managed the personal information of their customers pretty well. They practice fair information practices without maybe articulating that is what they were doing. As they bring new players into this environment, standards can set an appropriate benchmark for managing data. From the privacy community's perspective, we look at the smart grid as not just an energy delivery system but a huge communication network that will allow two-way flow of data between the home to the grid as well as communication among electrical appliances devices. So as they look to bring players in, how data might be used in ways that will enhance consumer trust and broader adoption of smart grid will have a lot to do with how consumer personal information or their energy usage data is managed in that system.

Chairman WU. Thank you for that point. It is that it is a communication system as well as a power delivery system that makes it a privacy as well as security concern and the fact that it is also not just energy storage but data storage ultimately for the smart grid that drives the privacy concern even further.

Mr. Smith, please proceed.

Mr. SMITH. Thank you, Mr. Chairman.

I appreciate all the testimony here, and I think that there are a lot of great points to be talked about. As I am meeting with con-

stituents here, back in my district and so forth, certainly I think it is fair to say that consumers are paying more attention relating to energy, electricity distribution and other things probably than in the history of our country. They are also paying more attention to what is happening here in Washington and they are concerned. The various trends that we see have them concerned. I mean, I point to a bill that we took up here not long ago relating to the social behavior of energy consumers. I would argue that any worthwhile economic study involves consumer behavior that should touch on some of those things as it relates to the economics and so forth. So I think we need to be mindful of that and make sure that anything we do is consumer-driven because that is I think that is more sustainable and more effective long term.

But that being said, we have a situation with the \$4 billion for smart grid technologies from the stimulus bill and I am not sure if there is a sign that says this is credited to the ARRA like so many of the projects around America do at a great expense to taxpayers, by the way, but I am concerned that we might have the cart ahead of the horse without the standards in place. Dr. Arnold, can you speak to how that money can be effectively spent in terms of utilizing and upholding standards that may not exist yet?

Dr. ARNOLD. Yes. Thank you, Congressman. This is indeed an issue that we have been paying very careful attention to for precisely the reasons that you have stated. One of the major areas of investment with these grants has been in smart meters and we recognized early on that some of the standards for the smart meters would have to be revised to accommodate certain requirements. So we tasked the National Electrical Manufacturers Association, which is responsible for developing the standards for the smart meters, to get the industry together and develop a smart meter upgradability standard and gave them a timeframe of 90 days to get that done and indeed that standard was developed and published last September with the full participation of the metering industry. So that is one example where we have thought about this and put in place a solution. Many of the other standards that we are talking about here on interoperability are based on software. They deal with information management and the ability to update software over time is well understood and part of the process.

Chairman WU. If anyone else wishes to answer, we will take your comments after we come back from votes. We are a little short on time now, and after Mr. Smith—after that answer, Chairman Gordon, Chairman of the Full Committee, will be the next to ask questions. The panel is now recessed until the completion of these three votes.

[Recess.]

Chairman WU. Thank you for your patience and forbearance on these three, four votes. Next will be the Chairman of the Full Committee, Mr. Gordon. Please proceed.

Chairman GORDON. Thank you, Chairman Wu, and thanks for having this very interesting hearing, and I want to thank our witnesses. You have been very helpful for us to better understand what is going on in the state of play now. I think we all recognize that a smart grid can help us become more—have more energy security, become more technically efficient, which hopefully then

means new markets for our new technology and jobs in those markets both globally as well as domestically.

But I want to follow up on a couple of things. Mr. McDonald, you had mentioned, and obviously you have a big stake in this in terms of products, that there needed to be international cooperation with the standards, and Dr. Arnold, you had mentioned that there were some collaboratives at different agencies, or not agencies but rather groups, as well as working countries. But I want to go back to a statement that you made in your written testimony and I would like to flesh it out a little bit more. I have read some reports that predict that China's preference for indigenous innovation will extend to the smart grid and that China may seek to establish its own standards for the smart grid in the belief that the size of its market will lead to their adoption as a de facto global standard. So with that sort of context, I assume this would not be a good thing for you, Mr. McDonald, as well as other domestic and global companies here.

So Dr. Arnold, you had mentioned that there is some collaboration going on. Can you tell me what is going on there and how your fears are now?

Dr. ARNOLD. Thank you, Chairman Gordon. I would be happy to elaborate on that. We are actively reaching out to our counterparts in China. NIST has hosted a number of visits by representatives from Chinese agencies including the state grid of China to discuss our standardization efforts. Several weeks ago a NIST delegation visited the Chinese National Institute of Metrology and the smart grid was one of the topics discussed. I have had meetings with the Chinese national committee to the IEC [International Electrotechnical Commission]. My deputy met a couple weeks ago with a Chinese representative to a new ITU-T [International Telecommunications Union-Telecommunications Standardization Sector] focus group on smart grid, and I and several members of my team at NIST have been invited to give talks at smart grid conferences in China and so we will certainly continue to engage in outreach.

What I can tell you is that China has publicly said that they intend to use international standards and for them, that primarily means IEC standards. One of the concerns that I have is that as we have learned through our process, there are about 27 different standards organizations that develop standards needed for the smart grid, so it is not possible to point to just one. Also, there are many instances in which countries will bring proposals into a group like the IEC and what is eventually adopted at the international level is not the same as the starting point and so there is a question as to whether if China does wish to pursue a different path on some of these standards whether they will indeed be harmonized with the United States and other countries. So we are going to continue to be very proactive in engaging in outreaching and establishing a dialog, and China obviously is a very big country with many players and I also believe that it is not entirely clear who has the lead within China on the development of the standards. So we are going to continue to work this intensively.

Chairman GORDON. Well, let us put China over to the side just a moment now. With the 27 different agencies, is there something

that we need to do in this country either legislatively, administratively to bring more continuity to that? And how is the rest of the world outside of China, how does that seem to be coming along with harmonizing?

Dr. ARNOLD. Well, with regard to the 27 different agencies, I think Congress has already in brilliant fashion dealt with that by enacting the Energy Independence and Security Act which gave NIST the role of coordinating, and that coordination I believe is going very, very well.

Chairman GORDON. But that is coordinating all of our efforts, but then you are having to coordinate in with all 27?

Dr. ARNOLD. Yes, coordination among the 27, and by the way, many of the 27 are international standards bodies. They include the IEC, the ITU-T. IEEE is really an international organization, and I would say the United States is really leading the way in terms of figuring out the architecture, what standards are needed, and getting the right discussions among all these players to produce the specifications that we need both in the United States and that other countries will need.

Chairman GORDON. So again, with China on the side, you are comfortable that the rest of the world is moving in a similar direction?

Dr. ARNOLD. I believe that we are. Clearly there are differences in the electrical systems around the world that have been around for 100 years and are probably never going to change, so it is not going to be possible to harmonize 100 percent in the electric grid, but a lot of the issues we are dealing with regard to information management don't differ, don't change whether you are operating at 110 volts or 230 volts and so I believe that harmonization is indeed possible—I am very optimistic about it.

Chairman GORDON. Any of the other witnesses want to bring any caveats or any thoughts to this issue? Okay.

And finally, is there any type of a WTO [World Trade Organization] or any type of a way to appeal if China were to go a completely different way for a proprietary reason?

Dr. ARNOLD. Well, if the result creates a technical barrier to trade that doesn't have some justification, I would assume that might be possible, but I don't know. We will have to see. I don't think China is far enough along yet. We are really leading the way in this standardization effort.

Chairman GORDON. Thank you.

Chairman WU. Thank you very much, Mr. Chairman.

Next, Mr. Broun, please proceed.

Mr. BROUN. Thank you, Mr. Chairman.

Dr. Arnold, is NIST ensuring that all smart grid standards are developed using a process that ensures a consensus that is consistent with the requirements of the National Technology Transfer and Advancement Act as well as the OMB [Office of Management and Budget] circular number A-119 that encourage Federal agencies to use standards developed by private consensus organizations?

Dr. ARNOLD. Thank you, Congressman. That is an excellent question, and, in fact, one that we discuss extensively in the SGIP, and because we are directed in EISA to use a consensus process and

FERC is directed to ensure that there is consensus, we have had to reach out for a definition of consensus, and the one that we have used is the definition incorporated in the NTTAA [National Technology Transfer and Advancement Act] and circular A-119. So that is sort of a foundation that we are using.

Mr. BROUN. So that is yes?

Dr. ARNOLD. Yes.

Mr. BROUN. Okay. Very good. Dr. Arnold, in light of the accelerated time frame and the numerous and varied organizations upon which NIST is relying to develop the smart grid standards, how specifically is NIST ensuring that all smart grid standards are being developed in a process that satisfies these strict requirements?

Dr. ARNOLD. Well, when proposals come up to include certain standards that are being worked in organizations that are, let me say—if you have an organization that is accredited by ANSI, it is pretty clear that it complies with the NTTAA and OMB. There are other organizations like the IEC or the ITU which operate at an international level which are deemed to be compliant with those principles because they are basically in their charter, but there is in some cases extensive discussions about the need to move some of the work that is going on in certain forums in the smart grid into more open processes and I can point to an example where the Zigbee Alliance has actually changed their process for public review and addressing public comments specifically because we insisted that it had to follow the principles in NTTAA and circular A-119.

Mr. BROUN. Very good.

Mr. EMNETT. EISA provides that FERC initiate a rulemaking once it determines that what is described as a “sufficient consensus” on standards exists. What criteria will FERC use to determine that sufficient consensus has been achieved and how will FERC independently confirm that such criteria have been satisfied?

Mr. EMNETT. Thanks for that question. It is a good question because we haven't yet gotten the first set of standards so the Commission hasn't spoken. It hasn't had to process the standards and identify the criteria that is going to apply in light of the processes that exist within the NIST standards development process. That said, on a staff level, we regularly engage with the NIST staff to monitor the development of the standards development process, the setting up of the Interoperability Panel and the working groups, and the discussion around the NTTAA and the OMB circular to make sure that we can advise the Commission of the progress that has been made within the NIST standards development process in terms of building that consensus and then ultimately have the record to present to the Commission once we get the standards.

Mr. BROUN. That is a big job and I trust that you all will fulfill it. How will FERC determine in its rulemaking process what smart grid standards will become mandatory and which will remain voluntary?

Mr. EMNETT. The statute directs FERC to adopt standards developed by NIST for which there is consensus in the NIST process provided that they relate to the interoperability and functionality of interstate transmission and regional and wholesale electric mar-

kets. The Commission in a Policy Statement last year interpreted that directive to apply to the breadth of electric facilities that involve smart grid interoperability. So that could include distribution-level equipment which would not traditionally be subject to the Commission's ratemaking jurisdiction and yet that is implicated in its smart grid jurisdiction through the approval of standards under EISA. The Commission also looked to the language of EISA to understand not only the scope but also the applicability and noted that the statutory language does not grant the Commission authority to manage or enforce standards under EISA. That said, the Commission does adopt and enforce standards developed by the North American Electrical Reliability Corporation, the North American Energy Standards Board, other standards development organizations that do present standards to the Commission for adoption under other statutes such as the FPA, the Federal Power Act. And so there will be an analysis that is required of each standard that is provided to determine whether regardless of the adoption under EISA there needs to be an incorporation of the standard into the mandatory regulations of the Commission.

Mr. BROUN. Thank you very much.

Mr. Chairman, my time is expired, and I have one more question for Mr. Emmett. I assume that we can submit written questions to be answered—

Chairman WU. We will do that, and also a second round.

Mr. BROUN. Well, unfortunately, I won't be able to be here to attend that, and I would ask unanimous consent to—

Chairman WU. Why don't we give you—why don't we ask unanimous consent for you to complete your questions?

Mr. BROUN. Well, thank you, Mr. Chairman, I appreciate that.

Well, then, Mr. Emmett, how will FERC deal with the standards that are applicable to facilities and entities that are outside its your jurisdiction?

Mr. EMNETT. FERC has interpreted the statutory language for those entities outside of jurisdiction or the activities that are outside of the Commission's jurisdiction, to mean that the adoption of a smart grid standard would not be mandatory or enforceable by the Commission. So there would be a distinction between the sources of jurisdiction for reliability matters or ratemaking matters under the Federal Power Act and the jurisdiction that EISA grants us in terms of responsibility to adopt the smart grid standards.

Mr. BROUN. Very good. Thank you, Mr. Chairman.

Ms. CONEY. I was wondering if I could add one point? The standards that are being developed, you are focusing a great deal on what is happening in the United States, but we also purchase power from Canada. There are concerns between Canadian and U.S. transfer of data and information so any standards that address the issue of stripping information from the electricity or power that actually flows across the border may present some additional challenges to international standards. I am not sure if that is part of any of the discussions that are happening with international standards organizations but there is concern about the data that is wrapped up in the energy that is actually moving back and forth across borders.

Mr. BROUN. That is a great point. I hope that Mr. Emmett heard your concerns, and I certainly share the privacy concerns that you do, Ms. Coney.

Thank you so much, Mr. Chairman.

Chairman WU. Thank you very much, Mr. Broun, and perhaps the panel when it is my turn to ask questions again could address the issue of how closely the Canadians and we are cooperating on the privacy side.

Mr. Luján, please proceed.

Mr. LUJÁN. Mr. Chairman, thank you very much. I appreciate the attention to the last mile, if you will, and it sounds like that is what we have been focusing on. The last mile I am referring to demand-side management. I want to make sure that we also don't depart too far from the importance of understanding what smart grid means to our distribution systems, our transmission systems, reliability, along those lines, and how it integrates fully as we talk about this.

How far off are we from establishing standards for the last mile, if you will, for the demand-side portion that it seems that we have been focusing on here? Dr. Arnold.

Dr. ARNOLD. Yes. Well, the customer domain which deals with the demand-side management is one of the major domains in the smart grid and our Release 1 Framework has a lot of standards that apply in that area, some of which are under development but will provide a rich set of tools for customers to get real-time access on their energy usage and be able to reduce energy usage both in residential, commercial and industry environments. So that is clearly a major focus of our standards effort.

Mr. LUJÁN. And Mr. Chairman, the reason I ask that question is, we have been engaged in installing rooftop PV [Photovoltaics] for some time, small wind systems for people with distributed generation, and we still don't have national interconnection standards. Here we are. It seems to me that had we had national interconnection standards, states that have adopted them have fully accelerated their installation of PV, securing the grid. Had we had a stronger, more robust system in New York when we experienced the blackouts and the brownouts, we could have prevented that if we would have had adequate distributed generation and some integration when we talk about large scale and small scale. It seems to me, Mr. Chairman, that we do need to fully accelerate when we talk about interconnection standards or standards associated with any application whether it is big or small with smart grid so that industry, which is driving this and making these investments, they can focus in and hone in on where these critical investments need to be, and so that is something that I am very interested in, Mr. Chairman, not only on the net metering side, which I think has an important component when we are talking about smart grid with bringing on and off, especially as you are going to be using the demand-side focus to maybe even firm up peak with what you may be generating on some small DG [Digital Generation] systems and be able to control that demand side in the home on a commercial application and then ramp up where you need to, which could prevent a peaking system from coming on. And so—

Chairman WU. If the gentleman would yield just briefly?

Mr. LUJÁN. Yes.

Chairman WU. I completely agree with the gentleman about the need for standards to connect distributed power sources, and with the assistance of former Chairman Boehlert, I drafted a small provision in an energy bill passed under Chairman Boehlert's leadership to make sure that some wind sources and other distributed sources could connect well to the grid. There was some question about NIST jurisdiction then and there was also some question about this Committee's jurisdiction but that is now well established. I yield back to the gentleman.

Mr. LUJÁN. I appreciate that very much, Mr. Chairman, and that is going to be an important item for us to solve and work with industry as well to make sure that we are able to come to this.

The reason I asked that question, Mr. Chairman, as well, is recently it was announced in New Mexico where there is a large effort, a partnership with Japan and the United States with a few of our national laboratories, with the city of Albuquerque, with commercial application with bringing in their smart grid technology as well. Japan as well, over the 1990s, have invested \$100 billion into this area, into this testing. They have been making significant investments into their distributed systems and transmission systems and have been concentrating on their last mile recently, which I am happy that they are coming with here, but as we look to see the companies that are coming in, companies like GE, companies like Portland General Electric to see what we can do with learning from the expertise that lies therein, to make sure we are including and we are collaborating with companies that have a strong presence in the United States as well with the integration into some of these test areas.

And so I certainly hope, Mr. Chairman, as we go forward that those are the kinds of ideas that we can definitely look to and that we don't forget about our brothers and sisters who are serving on the public utility commissions across the country. They have a lot to add, and I will tell you, Mr. Chairman, as a former regulator, that is a voice that we need to make sure that we are reaching out to, especially when we talk about these areas with the leadership over at NARUC [National Association of Regulatory Utility Commissioners] as well. So with that, I yield back, Mr. Chairman. Thank you.

Chairman WU. Thank you very much, Mr. Luján, and I just want to add that your energetic and intelligent participation in this Subcommittee is very, very impressive. Ms. Biggert and I were just chatting that the New Mexicans that we know, you and Mr. Heinrich and your predecessor, Mr. Udall, a lot of smarts there and maybe it is leakage from the two national labs that you have in New Mexico.

The Ranking Member—

Mr. LUJÁN. Mr. Chairman, if I may, we will take it for what we get it, sir, because it is hard to come by. Thank you for that.

Chairman WU. Ms. Biggert.

Ms. BIGGERT. Yes. Thank you, Mr. Chairman.

With regard to the smart grid, I really do appreciate the Administration's vision of a cleaner, more reliable, more efficient and effective electricity grid that creates jobs and reduces our dependence

on others. I have a couple of questions based on that. Let us start with the job issue.

It seems like there is going to be a lot of short-term jobs to do the installation but what happens to the meter readers? Are we going to lose more jobs than we will gain with this installation? Dr. Arnold?

Dr. ARNOLD. Sure. Well, I can tell you from the studies I have read, there was a study done by KEMA, a consulting company, about a year ago that estimated over the first several years of the smart grid deployment net gain of about 280,000 jobs in the United States, and in the long term they predicted 140,000, if my memory is correct, and what is interesting is that they actually analyzed the effect of the meter readers' jobs going away. There are about 42,000 of those jobs. So even after you subtract that out, their estimate was 280,000 net increase in the early years.

Ms. BIGGERT. But besides the installation, what jobs would be new jobs?

Dr. ARNOLD. Well, there are certainly jobs to do the engineering of these new grids, bringing in new technologies, the information technology and communications. These are new skills for most of the electric utilities and so they also represent opportunities to train a new generation of young people to pursue careers in the ongoing evolution of the smart grid.

Ms. BIGGERT. I have an article from Maine where they are concerned because those might be short-term versus the long-term a meter readers. They are concerned because of the stimulus was, you know, to create jobs, and it will, but will it be enough to overcome the long-term jobs?

Dr. ARNOLD. Well, the nature of the, you know, jobs to put in place the automation in the grid are long-term. I come from the telecommunications industry and a whole industry grew up through the automation that was done in the telecom industry in the 1970s and 1980s. Companies like Telcordia and many others found new businesses, and I think technology transformation is a wonderful way of creating new skills and new jobs that have a long-term nature.

Ms. BIGGERT. And then my district is home to the only Illinois recipient of stimulus funding. It is the city of Naperville in Illinois and it has about 145,000 residents, and it operates an independent municipal utility and they are just starting with using only wind power and biomass to create the electricity, so they are really moving ahead. But as the plans for their smart meter deployment move forward, a number of residents have expressed concern about privacy. So Dr. Arnold, can you tell us how feedback from the stimulus funding recipients will be incorporated into future standards development and would you really want to hear from all of these cities or whoever has the stimulus money and is creating these smart grids about standards? They probably—I think the discussion was before—that a lot of places are doing this but they really don't have the standards yet.

Dr. ARNOLD. Absolutely, so the privacy issues we regard as a key issue. We have a working group that is underneath our cybersecurity working group that is specifically focused on privacy, and I would like to thank Ms. Coney for being an active participant

along with many others in that. There is about 50 pages in the forthcoming NISTIR that deals with cybersecurity specifically on privacy and recommendations.

Ms. BIGGERT. Then Mr. Eustis, could you respond to the jobs question?

Mr. EUSTIS. Yes, ma'am. I grew up in Illinois, so I appreciate the Illinois connection. The jobs on meter readers, for example, we have been aware of this problem in our smart meter deployment. We have had two full-time people working to reposition the meter readers and we have now relocated 70 percent of the meter readers in other jobs within the company, so a focused effort there can, you know, put these people back to work.

But to the point of new jobs, there is an analogy if you look back to about 1986 to 1990 when we started putting computers on business desktops, and people were worried about getting rid of word processing groups, and yes, a lot of jobs were lost in admin assistants and libraries but I can tell you that the amount of IT support that now takes place to support all the utilities is like double or triple the number of jobs, and for example, the line workers today don't need any information skills. They are all going to need information skills in the future. We are going to need support tools. We need to maintain the databases. Customers as we get into the home are going to have questions and there are going to be support centers for people that answer questions. So while IT is supposed to make things simpler and makes it richer, it does require care and feeding.

Ms. BIGGERT. Thank you.

My time is expired. I yield back.

Chairman WU. Thank you very much, Ms. Biggert. The Chair recognizes himself for five minutes.

Ms. Coney, you referred in your written testimony a number of really unprecedented privacy concerns presented by smart grid development and its penetration right into the kitchen or other rooms in our home. How are smart grid technology developers and operators currently addressing privacy? Is this reflected in the standards that are being developed? And also, it is my recollection that you mentioned that you reached out to NIST and the standards process rather than vice versa, and I would like to ask Dr. Arnold to address whether NIST had reached out to other groups or whether in reaching out to other groups there was an oversight with the privacy groups. Ms. Coney, why don't you go first and then anyone else who wants to address this issue?

Ms. CONEY. Thank you. Privacy is basically on a fundamental level the ability of an individual to control who, when, why and how access to personal information is managed. So in the development of standards, we look specifically at the data that is being collected, as I mentioned earlier. Now, the incorporation of the knowledge of privacy experts into this process began with privacy organizations learning about the ability to participate in the cybersecurity subgroup on privacy. We brought to that discussion some perspectives that were not resonant inside of the process initially, but through the participation of privacy cyber there is knowledge at NIST about privacy issues and the smart grid. They produced a document actually in April of this year that is titled

“Guide to Protecting the Confidentiality of PII,” which speaks to a lot of the key components of privacy. In standards development, we should focus on how do you give consumers control over the information about their electric utility usage. Control can be as simple as an interface device for existing appliances that smart adaptors that connect appliances to electric outlets customers plug the appliance into that interface device that allows the micro management of energy consumption on the consumer level, Giving the consumer access to information about the peak cost hours versus the low-cost hours to run very energy-intense devices; and as customers purchase new appliances and technology to replace worn—out or broken equipment that the same level of control of energy consumption data confers to these new purchases.

As far as the participation in the NIST process is concerned, advocacy groups and NIST just don’t swim in the same waters. I happen to be more aware of NIST because I work on technology issues regarding voting systems and its standard development process. But I must say that NIST has been open-minded about privacy advocates’ our participation, while still not quite sure how it is hard science. We have worked very hard to make sure that NIST, utilities, and others understand that the principles of privacy are grounded in fair information practices and that those practices can be conferred into architecture designed software applications that give consumers control over their personal information.

Chairman WU. Well, Ms. Coney, as technology develops further and further and has further implications for our privacy and personal behavior patterns, perhaps this Subcommittee or this Committee can provide the encouragement to NIST to swim further in other ponds, and I also want to underscore that in this new arena, it is not just when devices are coupled with communication or wireless technology. I think there are several competing technologies currently incompatible, I understand, to send information back out over the power wire. So, you know, there is a lot of chatter that is going to go on.

Dr. Arnold, would you care to toss in just a little bit on this question?

Dr. ARNOLD. Sure. Well, we are well aware that the smart grid touches everyone and many constituencies that haven’t been thought about in the electric system and we are not omniscient so we can’t possibly know everyone who we should be reaching out to but we have really tried to make our process as open as possible. We have made use of the Federal Register. Our website provides collaboration opportunities. We have tried to get as much word out through the process, through industry associations.

In terms of your question as to whether we specifically reached out to the privacy community or whether they reached out to us, I will have to reach that and—

Chairman WU. No, the question is whether the privacy groups were an outlier and you reached out to a bunch of other folks and not them.

Dr. ARNOLD. I will have to—I want to give you a precise answer so I will have to get back to you with what outreach we may or may not have done in that particular case.

Chairman WU. Terrific. I look forward to it, Dr. Arnold.

And Mr. Emnett, I just want to comment that as important as voluntary standards are, in the privacy area, there are always some outliers, so I think that FERC will have an important role once the appropriate standards for policy and other purposes are developed.

Mr. EMNETT. If I may, Mr. Chairman, the Commission did recognize the importance of cybersecurity in our Policy Statement where we identified the criteria that we would apply to standards when they come in, and in light of the emphasis on cybersecurity in the Energy Independence and Security Act, we did state that we would require a showing of adequate cybersecurity protection prior to adopting any standard under EISA.

Chairman WU. Terrific. I just want to add that there is the cybersecurity issue. There is a concern about privacy and perhaps there is a related but different concern about anonymity, and anyone who has purchased, for cash, stuff at the grocery store understands the separate nature, that third component, not that any of us have concerns about that. We just may not want Safeway to know what we are buying.

Ms. Biggert, back to you.

Ms. BIGGERT. Thank you, Mr. Chairman.

Dr. Arnold, the decisions that NIST makes with respect to the numerous standards will probably and most likely be picking winners and losers among competing standards with the companies that own the intellectual property that support the standards, and so they are set to make or lose millions of dollars based on the outcome of your process. How are you working to ensure that the standards finalization process is open and fair and transparent?

Dr. ARNOLD. Well, NIST does not want to be in the position, nor should we, of picking winners and losers. No, I view our role as accelerating a process that primarily involves industry with government as an important stakeholder to accelerate the normal industry process of winnowing out the winners in the marketplace. So some of these standards might have taken five or ten years before it became clear and in the meantime there is confusion and people are afraid to invest. We are trying through our process, to get all the stakeholders together to more rapidly reach consensus and not be in a position where NIST is picking winners and losers.

Ms. BIGGERT. But it does come into the intellectual property, doesn't it, or what their proprietary—

Dr. ARNOLD. Yes, indeed. So the earlier discussion on the NTTAA and OMB circular A-119 is very important because that does include requirements that intellectual property that is needed to utilize the standards be available on reasonable and nondiscriminatory terms to anyone who has a need to practice the standards, so that is one of the fundamental principles that we are following.

Ms. BIGGERT. Thank you. I yield back.

Chairman WU. Thank you very much, Ms. Biggert.

Mr. Luján.

Mr. LUJÁN. Thank you, Mr. Chairman, and the reason for the line of questioning around net metering and interconnection standards that we could establish nationally based on IEEE standards would ultimately lower cost, and I appreciate the line of questioning from our Ranking Member as well looking to see what the

role is with NIST and how we can work with private industry to drive the standards on the plug-and-play, if you will, nature of what we are talking about here, the interface. With that being said, hopefully, Mr. Chairman, maybe one day we can tackle a hearing on how we can have a set of chargers for our mobile phones that are all the same and we don't have to keep buying them every time we get a new phone, but I think that is a conversation for another day.

Looking to see what we can do, and Mr. McDonald, I think I will start with you here, sir, what can we do to be working with our national laboratories as we talk about intellectual property, tech transfer, commercialization, maturation, maybe refining the technologies that you have where we can take advantage of supercomputers or simulation and modeling capabilities that no one else has, which is truly a competitive advantage that United States companies have? What more can we do along those lines to open up opportunities, for example, with GE for you to work with our scientists and physicists along those lines?

Mr. McDONALD. Well, that is a very good question. I think we—you know, we have to make sure that in addition to the standards process that we continue to spur innovation. Some people think that standardization squashes innovation from the point of view of everything looks the same, and it is very different than that. When we—you know, when we implement standards and products, it is true that a family of products will have the same functionality, core functionality, but it is the differentiating features that each supplier has that extends the standards model basically. So we can have a win-win situation of having standards but still have innovation. I really think with smart grid, you know, the emphasis on smart grid is not to implement technology that we have been implementing in the past. We really have an opportunity to innovate, and what we say really is that what we have been in the past is device level and system level, and with smart grid we have a whole new level of innovation which is solution level. How do we put together devices and systems that we haven't done before to provide solutions for customers, and this is where the innovation takes place, and we need to—you know, the national labs are very much involved with the NIST process, and we need to continue to spur that innovation and have that input. So, you know, once we have the innovation and the technology, then the next step is the commercialization step so that what we have from the labs or from research is usable by electric utilities, the end-use customer, and there is a commercialization step that needs to take place there.

Mr. LUJÁN. I appreciate that very much.

Mr. Chairman, and I know that both yourself and Ms. Biggert are big supporters of our national labs and with tech transfer and innovation to see what we can do to truly engage in that dialog to have that push and pull effect of the technology.

Along those lines, Mr. Emmett, with FERC looking at this and along the lines of what we may be able to do, and Mr.—is it Eustis?

Mr. EUSTIS. Yes.

Mr. LUJÁN. I would like to hear from you if we get a chance as well. With the integration of what we are talking about with broadband and they have been testing broadband over power lines

for some time, looking to see what we can do with some of our superconductors now with new transmission, paths that are going to be built in a country and DG lines that are going to be built out as well, what can we do for the integration of fiber or whatever other means are necessary to increase our capacity for communication or is it truly integrating with our telecom companies or cable companies, whoever it may be supplying that last mile of fiber? Because of the infrastructure associated with electric companies specifically, it seems to me that we have many of the easements needed that are going right to the home where we could provide that more robust deployment of broadband application. Any thoughts along the lines of what FERC is looking at there with the inclusion of the cyber application and cybersecurity needs?

Mr. EMNETT. Yes, I think it could be possible that under the particular state regulatory structure that there are mechanisms in place to allow companies to essentially leverage the existing investment and access the home. And in terms of FERC'S interaction in the standards development process and the facilitation of the technology development to make that happen, we have tried to identify our priorities within the standards development process, one of which did include demand response, other electric storage, plug-in vehicles—priorities that from the Commission's perspective development of standards to address those applications would facilitate and support national energy policy, and then once we identified the priorities we essentially handed it off to NIST which did we think just a great job of addressing the priorities in their standards development process, adding their own priorities and driving towards the creation of the priority action plans to address the gaps in existing standards so that there can be standardization, not necessarily in the results or the products but in the processes, as Mr. McDonald was saying, so that the technological innovation is essentially facilitated.

Mr. LUJÁN. I appreciate that. I know my time is expired, sir, so Terry or someone from my team, Mr. Eustis, will get in touch and we will talk about that later.

And then Ms. Biggert, with the line of questioning around the number of meter readers that may be impacted, that is an important aspect of this, because one thing that we do know with utility companies across the country is the workforce is aging as well and we are not replenishing, so I think a whole conversation around what we need to do to be making sure that we have adequate recruitment around making sure that our utility companies are going to be in a strong position in the near term and long term is something that is critically important, so I appreciate that perspective very much.

Ms. BIGGERT. Would the gentleman yield?

Mr. LUJÁN. Yes.

Ms. BIGGERT. Don't you think, too, that there is going to have to be a lot of training for much more skilled workers? And I think that is good. I think technology demands that.

Mr. LUJÁN. Ms. Biggert, I could not agree more. I appreciate that.

And with that, Mr. Chairman, I yield back my time.

Chairman WU. I want to ask unanimous consent to insert in the record a statement from Vinton Cerf, the Vice President and Internet Evangelist for Google. These high-tech folks are very creative. Without objection, so ordered.

[The submitted statement of Dr. Cerf follows:]

SUBMITTED STATEMENT OF VINTON CERF

Dear Mr. Chairman,

This letter is in response to a recent informal discussion I had with Committee staffer Meghan Housewright about the challenges and opportunities implicit in the Smart Grid standards facilitation effort now under way in the United States under the auspices of the National Institutes of Standards and Technology.

For the benefit of possible readers of this letter, I thought a little capsule summary of my interests in this matter would be appropriate. My name is Vinton G. Cerf and I serve as Google's vice president and chief Internet evangelist. I am the co-inventor of the TCP/IP protocols and architecture of the Internet. I also serve as the chairman of the Visiting Committee on Advanced Technology for the National Institute of Standards and Technology (NIST) and as a member of the Smart Grid Interoperability Panel Governing Board. Google is an interested party as well through its development of the Google Power Meter (hardware and software system).

The lead U.S. Government program manager for the Smart Grid program is Dr. George Arnold who is the National Coordinator for Smart Grid Interoperability and reports to the Director of NIST, Dr. Patrick Gallagher. I have had the opportunity to work and interact with Dr. Arnold over the course of some years in connection with my responsibilities at NIST and, more recently, in connection with the Smart Grid Interoperability Panel (SGIP). I want to go on record to say that Dr. Arnold has undertaken an extremely difficult and complex task: facilitating the development of standards needed to assure that the vision of a smart grid can in fact be realized. Moreover, the level of interest in the program is easily illustrated by noting that the SGIP activity now involves on the order of 600 companies and 1600 representatives. The organizational structure and governance mechanisms of the SGIP were created quickly and formulated for maximum flexibility as a non-profit, private sector organization. Dr. Arnold deserves great credit for his successful efforts thus far.

Perhaps even more important than the institutional aspects of the work is the vision and motivation for the development of a "smart grid." I do not propose to outline this vision in its entirety in this brief contribution, but plainly there are many reasons for pursuing this course. If we can make more efficient use of electricity and avoid excessive use during peak load periods, we can avoid unnecessary capital investment and operating costs. To do this, we need appliances and mechanisms that will allow consumers to adjust their use of electricity in accordance with their preferences in more or less automatic ways. This means that our energy consuming appliances need to be able to communicate with the power grid management system and with each other. To achieve this goal, standards are needed, as has been admirably articulated by Secretary of Energy Steven Chu and Secretary of Commerce Gary Locke.

The Smart Grid program is also partly motivated by the potential for job creation since new appliances will be needed as well as new monitoring systems, power meters and the like. Their production in quantity will lead to job growth in the appliance, power generation and monitoring sector. There is tension between the need for standards and the opportunity for job creation, however, because establishing standards for such a massive and complex undertaking needs time while job creation is a matter of urgency. Investing huge sums in the production of appliances using inappropriate standards could lead to serious vulnerabilities and fragility in the evolving 21st Century power grid. This tension makes the results of the SGIP initiative all the more important to get right.

In forming the Smart Grid Interoperability Panel and its Governing Board, Dr. Arnold has drawn upon a diverse, motivated and well-qualified cohort of participants. The structure of the standards effort involves nearly two score Priority Action Panels, several Working Groups (especially on Security and Architecture), and a number of ad hoc review groups. I cannot over emphasize the importance of the Architecture and Security working groups. If the effort is successful, the new power grid will allow appliances to reduce demand at the discretion of the consumers. Until now, the power grid has had to meet demand or be forced into rolling "brown-outs". It is a tribute to the power industry that it has managed in large measure

to meet the growing demand for electricity in the United States. However, a poorly designed software architecture or inadequate attention to security could create an unstable and unreliable system. Such an outcome would surely represent an unacceptable national security risk. One of my colleagues in the Smart Grid Interoperability Panel has also reminded me that the grid is not only vulnerable to potential software hazards but also to a range of physical frailties, exacerbating concerns for reliability and robust operation.

Without reprising all of the many discussions that have taken place in connection with the frequent SGIP meetings, perhaps a few points are worth mentioning:

1. Standards will permit power meters and energy monitoring systems to interwork with appliances and with the power grid's management systems.
2. Open, non-proprietary standards promote competition because multiple parties can make equipment that will interwork without having to make pairwise agreements or be limited by licensing requirements.
3. Properly testing standards and their implementation can reinforce the security of the Smart Grid systems.
4. Standards suitable for international use can increase markets for American-made appliances.
5. Information from energy usage monitoring can reinforce consumer awareness of the consequences of their energy consumption. Consumers should have full access to this information and be empowered to provide it to third parties for analysis.

Among the most significant challenges in this Smart Grid enterprise is the introduction of power generation in residential and industrial settings. While co-generation has been around for some time in the latter, the introduction of photovoltaic or wind or fuel cell power generation in residential settings is relatively new. As the economics of such distributed generation improves, there is increasing interest in local power generation and consumption. For the first time, consumers have the potential to become producers. Plug-in electric cars add to this picture as potential sources and sinks of electrical power. This phenomenon has both benefits and risks. On the beneficial side, use of renewable energy resources can reduce our dependence on non-renewable fossil fuels and potentially reduce the production of atmospheric carbon dioxide, a greenhouse gas. In addition, reduced use of fossil fuels can also reduce our need to import energy sources, improving our trade balances. On the risk side, for most of the history of power generation in the United States, the power grid has used large-scale, centralized power generation facilities and an extensive power grid to deliver electrical energy to consumers. As power generation becomes more distributed and its sources more variable (wind power and photovoltaics operate episodically and not continuously, for example), the stability of the power generation and distribution systems becomes an even larger challenge than before. When we add to this mix the use of smart appliances that moderate their demands, we have a very complex, dynamic control system problem to solve to assure that the system stays stable.

From the national security standpoint, the nightmare scenarios include the potential for a large number of appliances to simultaneously turn on or off, either because of common algorithmic decisions (think: programmed trading in the stock markets) or because someone has penetrated the power control system or somehow induced a large number of appliances to act in concert. Of course, there is also the ever-present possibility of human error or bugs in software that lead to the same effects. These concerns only reinforce the importance of care in the development of the standards and in careful analysis of the security provisions in their design. That the system must be resilient in the face of natural disasters is also apparent. Software alone will not prevent an ice storm from breaking power lines or prevent a hurricane or tornado from damaging a power plant or substation.

Another of my fellow SGIP Governing Board members has pointed out that the decisions and choices we make in the design of the Smart Grid standards may look arbitrary at the outset but may prove to be utterly crucial in the long run. Since we cannot be certain which choices have this property, he strongly recommended that we devote the necessary time and resources to make use of testing, modeling and analytical methods, including prototyping, to assure that we have identified the not-so-arbitrary choices early on in this process. The Governing Board has strong advocates for a testing and certification program that would assure consumers that standards are met in the devices and appliances placed on the market. I support that view and extend it to include early testing and prototyping to avoid making large investments in dead-end designs.

In the course of the many discussions about the Smart Grid idea, the question of fine-grained information as to usage and pricing has arisen. Fine-grained time information about pricing and usage can be used to moderate consumption and reduce peak load demand. Just how beneficial this may prove to be is still an unknown, at least as I comprehend the idea. Real data is needed to inform any credible opinions and this motivates once again the need for prototyping and pilot programs of use. I am told that fine-grained pricing information is not uniformly available at the retail level although it may be provided to wholesale customers who may be trying to minimize their costs by drawing on different suppliers at different times.

While on the subject of fine-grained usage information, I think it is useful to remember that much can be inferred from such profiles. One could likely know whether someone is at home, possibly even who might be at home if one knows which appliances are in use. Diurnal patterns of usage, accumulated over time, could be used to identify periods when a home is unoccupied. Plainly there are privacy, safety and security issues associated with access to this information. With regard to access, it seems important that consumers have access to and some control over who may have access to this kind of information. Consumers may want third parties to have access for analytical purposes but at the same time assure that the information does not fall into the wrong hands.

As should be obvious from this brief letter, the development of the Smart Grid is by no means a trivial enterprise and has many facets of interest to a wide range of policy-making bodies, private sector actors and, of course, the general public.

I commend the Committee for its continuing interest in improving and evolving the American response to the need for more efficient production and use of electrical power. I hope that this same attentive perspective will be given to other resources of importance. If we design the standards for the Smart Grid well, they can be extended to monitor our use of water, oil, gas, and other resources, giving all of us a better sense of the consequences of our life style and resource consumption choices.

Vinton G. Cerf  
VP and Chief Internet Evangelist  
Google

Chairman WU. The chairman recognizes himself for another five minutes and I understand that Ms. Biggert has a conflicting obligation. Thank you for taking the additional time.

Mr. Emnett, you mentioned in your testimony that FERC intends to allow utilities certain smart grid-related costs if certain factors can be shown, and one of them is that the applicant is to show that it minimized the possibility of stranded investment in smart grid equipment. We are in the process of developing the applicable interoperability standards so how is FERC going to proceed in making this determination? And Mr. Eustis, I guess I would like to hear from PGE's, Portland General Electric's perspective how you feel about stranded investment recovery versus not?

Mr. Emnett, you first.

Mr. EMNETT. Sure. In the Policy Statement that FERC issued last year, FERC stressed that it would look towards applicants seeking to recover the costs of smart grid development prior to the adoption of related standards. It would expect the applicants to make a demonstration that, to the extent possible, they are relying on whatever existing open standards may be out there—so not necessarily those that have been adopted by FERC but those that are generally followed by the industry—as well as a demonstration that the equipment and technologies that are being invested in can be readily and securely upgraded. The Commission has had one instance of a utility seeking confirmation, affirmation of cost recovery under the Policy Statement, Pacific Gas and Electric, incorporating costs associated with development partially funded by the Recovery Act, the other PGE, PG&E [Pacific Gas and Electric Company], not

PGE. So Pacific Gas and Electric did in fact make the demonstration that they were being careful in the selection of the technologies, that they tested different product vendors, component testing for ease of integration, implementation of open modular architecture for the facilities. So there was a demonstration that the applicant was able to make that the technologies would be flexible in the event that standards were developed in a different direction.

Chairman WU. Mr. Eustis, you bear the burden of representing all utilities, so from the utility perspective, how is it going in terms of the risk-reward on proceeding and the risk of stranded costs?

Mr. EUSTIS. So, as we planned our business case for smart meters, for example, we definitely considered future applications and making sure it wouldn't be obsolete but first and foremost the business case has to be cost-effective that we implement and so the functions that we built the technology for are implemented and will be functional for the economic life of the project, so the first thing is make sure what you are investing actually serves an economic purpose.

As far as interoperability over time, we look to things, technical hardware like communication bridges to bridge one protocol to another for those customers that need it, or the upgradeable firmware in a meter or in a distribution switch allows us to add additional functionality when the time comes. So the most important factor to prevent stranded assets is making sure that there is an upgradeable path to the hardware that you install.

Chairman WU. Ms. Coney?

Ms. CONEY. I would like to add for the benefit of consumers that their stranded costs should be considered as well as they purchase new appliances, whether there will be additional costs incurred as new software, new hardware, new applications are placed onto the grid, will it push consumers to have to make additional expenditures. Human user interfaces for consumer devices and appliances should allow users to control or manage energy usage within their home. Energy consumers must have a full range of options for how their energy consumption will be managed. Control should not be pushed out of their control because of the design of devices and appliances based on the standards which are developed. Consumers should have a range of options for how to manage energy consumption.

Chairman WU. Ms. Coney, I will view this as the request to give hope to those who still have eight-track tape players and beta video machines.

Ms. CONEY. Privacy advocates typically like technology or those who like to be first adopters and like to tinker. Vint Cerf happens to be on EPIC's advisory board. He is one of the people who could appreciate having the ability to have the option for managing or not managing their own electric utility usage. Thank you.

Chairman WU. Thank you, Ms. Coney, and that makes me feel better because the young people around me always make me feel like a Luddite in adopting new technology, but I think that is just commendable caution for those who have seen many things come around.

A further money question. The NIST budget includes \$10 million for standards and conformity assessment. This initiative will cover

some smart grid activities as well as other technologies, and Mr. Arnold, this is the one you can go to town on. What resources do you think NIST will need to appropriately develop standards at a pace which I think the industry and our Nation needs? And if additional resources were appropriated by this Congress, what additional activities or what delta and speed could you achieve?

Dr. ARNOLD. Well, if there were additional resources, my view is that the testing and certification program is the area that is in greatest need. As I think someone observed earlier, the standards in terms of the descriptions are necessary but they are not sufficient. Where the rubber meets the road is where you formalize the conformance requirements and the testing. There are hundreds of standards. There are many test programs that will be needed. We have efforts underway to develop a framework for that but getting these programs instantiated and in operation is going to be a big task, so I think that is the area in which there is the greatest need.

Chairman WU. Additional resources, additional activities, additional speed? I know you are trying to be a good foot soldier for the Administration but the question is asked.

Dr. ARNOLD. If there were additional funds available, they would be well utilized. Most of the testing programs will be done by the private sector but the development of these programs today is done largely on a voluntary basis, and to the extent that funds can be utilized to apply more full-time dedicated resources, the availability of these programs would be accelerated.

Chairman WU. Mr. Arnold, we will apparently take this up offline, but if any of the other panelists would care to take a poke at this question, your comments are welcome.

Ms. CONEY. I would offer that if we look at projects and their implication for being done well, I look to the Panama Canal as the last major engineering effort that continues in use today. The United States delved into the project and took the lead on following the French effort. It was an engineering marvel. It cost to do it right. And if we plan to do a smart grid, and with the consequences to cybersecurity, individual privacy, reliability, energy independence and all of the best wishes for the smart grid, it will need to have appropriate investments made in critical areas regarding standards development, the time and energy of the legislative branch in developing policy that assures that all of our best hopes of privacy and security regarding the smart grid are realized.

Chairman WU. Well, let the record show that it was the NGO advocacy organization that jumped in with both feet on this one.

Mr. Tonko.

Mr. TONKO. Thank you, Mr. Chair, and thank you to our panelists. Obviously one of the big changes out there that I think we need to incorporate and focus on are electric vehicles, and Dr. Arnold, in your testimony you discussed the fact that there are at least four competing proposals for the fast charging of electric vehicles, and my question is about the uncertainty that this might foster, that if we slow down that development, I think it is to the detriment of our comprehensive energy plan if we indeed have one, but I think our Nation should build that sort of plan. How do you think this issue is being addressed and how it is best addressed?

Dr. ARNOLD. Well, this is a complicated issue. I was in Japan a couple weeks ago and saw a demonstration of a system that is deployed on a pilot basis there, and I also had spent some time with the deputy CEO of the electric utility in Singapore, which is going to be piloting a similar system and they are actually requiring changes to the Japanese system for deployment in Singapore. So this is an area in which I think there is still some technical debate that needs to be engaged and we do have to balance speed versus doing this right. But at the end of the day we do need to make a decision on a single charging infrastructure standard for the United States because otherwise it is not going to be practical to develop the market for electric vehicles.

We are actively engaged with the key standards bodies in which these areas are being debated including SAE [Society of Automotive Engineers] International and the International Electric Technical Commission. One of our priority action plans is on electric vehicles and this issue is part of that. One of the debates that is occurring among these competing proposals are the safety aspects, and when it gets to safety, we want to make sure that we are doing this right. So we are working with these bodies to convene a workshop to get the experts together to discuss the safety issues and inform what I hope will be a decision by the end of next year on a standard for use in the United States.

Mr. TONKO. Is there anything you envision the Congress doing in the interim? Is there an incentive that needs to be developed? Is there some sort of effort that can be toward the single charging infrastructure?

Dr. ARNOLD. I mean, the only thing that I think would help would be sort of clear direction that there has got to be one. This is not an area in which you can have cars that have different sockets and charging levels going around the country. We need one standard. My guess is that internationally there won't be a single standard in much the way that we haven't standardized left-hand drive versus right-hand drive in different countries, so there will probably be two or three as we look around the world and they will be embraced in some sort of umbrella international standard. But for the United States, we have to pick one, and just making clear that we can't have a proliferation of different competing approaches in the marketplace would be helpful.

Mr. TONKO. And in your review of those areas around the world where you have witnessed their progress, anything gleaned from that that you would suggest to us as maybe an essential?

Dr. ARNOLD. I think that we need a lot of real-world experience on how consumers are going to react to these vehicles, the issue of driving range, how to deal with this. We are into an exciting new area here but one in which we really need some real-world experience to see the right way for this to evolve.

Mr. TONKO. Thank you very much. Mr. Eustis.

Mr. EUSTIS. Portland General Electric is lucky enough to have one of the early implementations of electric vehicles in its service territory with the Nissan and state partnership, and we got that opportunity because we put infrastructure out initially. It didn't need a standard but we designed the charging infrastructure in a way that could be upgraded later on, you know, the right conduits,

the right information support to that, and in much the same way the fast charging can be upgraded if a standard should change. I agree with Dr. Arnold absolutely, you know, one socket is what is required, but in the short run, the 240-volt standard, which is SAE 1772, I believe, does standardize, I think it is worldwide even, a method for the most predominant method of charging, and so the first order of business is to make sure we successfully get customers to adopt electric vehicles and the 240-volt standard will go a long way to get the early adoption and it gives us a little time to perfect fast charging.

Mr. TONKO. And Ms. Coney?

Ms. CONEY. The one thing I would add is that there have been discussions about whether the identification information for a unique electric vehicle should convey when that vehicle is being re-charged. The privacy perspective, especially as it weighs on the fast adoption of these vehicles, would be to make sure that re-charging is anonymous as paying with cash. Where you charge a vehicle should not identify that you in fact were in a particular place. There are privacy issues with architecture that supports transferring that kind of information in the process of charging an electric vehicle. Thank you.

Mr. TONKO. Thank you.

Thank you, Mr. Chair.

Chairman WU. Thank you, Mr. Tonko, very thorough, as always.

Mr. EUSTIS, you commented on the implementation in Portland for charging electric cars, and I asked a couple of questions of the company that is building out a charging field, if you will, or, you know, reaching from Portland to Salem or beyond, and their statement was that their charging format for the Nissan Leaf is not necessarily compatible with the Tesla that is sold more in California, or at least I have seen it in Silicon Valley a lot, and my comment back to them is that they are going to get a whole lot more enthusiastic support from Elon Musk and others if there is a compatible plug, and I just wanted to flag that because there apparently is a disagreement or not complete agreement about whether it is compatible or not. And you don't have to comment right now if you—

Mr. EUSTIS. Yeah, I am not familiar with that technical difference. I don't doubt that there is. But it would be at the fast charging level.

Chairman WU. Well, it may be just like really, I mean for a guy like me, really basic like three prongs versus two and those adaptor plugs that we fiddle with all the time.

On international standards, and again, if you all want to consider this and answer on the record later, or if you want to answer this, take a stab at it right now, I am concerned as Chairman Gordon pointed out about certain countries, particular China, in this field as in others developing their own standard to create an island of technology, whether that is for very legitimate national reasons or whether it is for trade and competitive reasons. Is there anything that we can do at the international standards-setting level or with other mechanisms available to us to provide both carrots and sticks for international cooperation and harmonization of standards?

Dr. ARNOLD. Chairman Wu, that is a very thought-provoking question and I would prefer to respond to that on the record later after giving it some consideration, but I think that this is a difficult issue. Where we have partners that recognize that the market grows. If you have common standards and you can create new industries and applications, it is easier. Where you have partners that view this as a win-lose game, then it is more difficult and it takes two to tango, as they say.

Chairman WU. Well, Dr. Arnold, I very much appreciate you taking the time and energy to answer in a thorough and careful way. It is NIST's mission to cooperate internationally, and this is what this Subcommittee has pressed for repeatedly, and if NIST or any other governmental agency needs carrots or sticks, I think that this Committee will seek to give you those tools.

If no one else wants to comment on that, you all have come—many of you have come from a long distance and it is the tradition of this Subcommittee when time permits to ask of the entire panel individually, are there things that we have not asked or that you have not had an opportunity to address live that you would like to address before we adjourn? Mr. McDonald.

Mr. McDONALD. I wanted to—there were two points that I wanted to cover. One was that Mr. Luján brought up about the importance of state regulators, and the fact that standards are really tightly tied to policy and vice versa. There is a lot of interdependencies. We realize that at NIST, and we made a conscious decision for our next Governing Board meeting next month, or actually this month—today is July 1st—in a couple weeks to be co-located with the National Association of Regulatory Utility Commissioners Summer Meeting in Sacramento, California, so all of the NIST Governing Board will be meeting together with the NARUC Commissioners, and our meeting will be open. All the commissioners can attend our Governing Board, and likewise the next two days, the NIST Governing Board will be involved in the regulators' meetings also. So we see that as important and we have reached out to NARUC and decided to have our meeting co-located with theirs.

That was one point. The second point was the permanence of jobs I think really boils down to standards. You know, if the technology is anchored in standards, it has permanence to it, and as a supplier, when we commit funds to incorporate new technology, if that technology is not anchored in a standard, there is a question from the supplier point of view is if we implement, commit resources and implement, that technology may go away the next year because there is not the stability to it that a standard provides. So I think, you know, with respect to technology, with respect to smart grid, with respect to jobs, it puts even more importance on standards. The more we have standards, the more we can interoperate, the jobs that we create with respect to smart grid will be permanent jobs. Thank you.

Ms. CONEY. I just wanted to close—

Chairman WU. Let me just respond to one thing that Mr. McDonald said about the permanence of jobs. We have a competitive society and also those of us who sit on this side of the dais completely understand that the functions of society may last for a long time but no job is permanent. Certainly no job is permanent.

Ms. Coney, please proceed.

Ms. CONEY. Thank you. I wanted to thank the minority for the invitation to participate in today's hearing. I think this is a very topical discussion but we didn't touch much on the topic of cybersecurity which from our perspective has a lot to do with data collection, retention and use but that the standards process can greatly benefit from the collaboration with privacy experts, civil liberties experts as well as legal experts on the consequences of the data collection and use related to smart grid. We hope that the consumer as the end user is taken into consideration when standards are developed to be sure that their interests are served as well. Thank you.

Chairman WU. Any other comments for the good of the order? Well, thank you all very much. Ms. Coney, I am really glad you mentioned the Panama Canal as the last great engineering project of this Nation. Perhaps that is true, but it certainly permits me equal latitude in using something dramatic. To borrow a Churchillian phrase, this is a really, really important project and yet it is very, very complex and abstruse, so a lot of the general public, and in fact, a lot of this legislative body, is not going to understand the process as it goes forward, but it is absolutely vital to our energy security going forward, and to borrow a Churchill structure, if not his words, never have so many depended on so few to take on a topic so important and to get it right, and I thank you for your efforts to date and offer this Committee's support, continuing support to get it right going forward.

And with that, the record will remain open for two weeks for additional statements from Members for answers to any follow-up questions the Committee may ask.

Thank you all very, very much for your participation. The witnesses are excused and the hearing is now adjourned.

[Whereupon, at 12:27 p.m., the Subcommittee was adjourned.]



## Appendix 1:

---

ANSWERS TO POST-HEARING QUESTIONS

## ANSWERS TO POST-HEARING QUESTIONS

*Responses by Dr. George W. Arnold, National Coordinator for Smart Grid, National Institute of Standards and Technology*

**Questions submitted by Chairman David Wu**

*Q1. In your testimony you mention that NIST is initiating a contract to develop cyber-security testing requirements for smart meters, and that the testing protocols should be available about a year after the contract is awarded. When will this contract be awarded? What concerns are there with deploying smart meters that have not undergone this testing and evaluation?*

*A1.* The proposals are currently under review by NIST and follow our Federal acquisition process to award based on contractor capability and best value. NIST anticipates awarding this contract before the end of this Fiscal Year.

*Q1,1a. There have been stories in the media from California and other places around the country about smart meters that do not function properly. Would a testing and evaluation program have identified problems with the meters before they were deployed?*

*A1,1a.* It is unclear whether the problems reported in California, Texas and other places are due to technical problems with the meters.

At this time the main concern with deploying smart meters that have not undergone interoperability and cyber-security testing is the potential for lack of interoperability and potential for security vulnerabilities that could compromise the meter. NIST is aware that a number of major utilities have labs that are testing vendor products prior to their selection and deployment and are providing feedback to the vendors on problems uncovered during their testing. Unfortunately, we understand that the results of these tests cannot be shared with other utilities, NIST, or other parties due to non-disclosure provisions in vendor contracts; therefore, NIST cannot comment on what problems have been uncovered through testing. The work that NIST is contracting for will result in a well-defined and consistent test methodology that can be broadly applied by accredited test labs to support the industry. NEMA Standard SG1 for Smart Meter Upgradeability, published in September 2009, was one of the first Smart Grid standards to be developed through the NIST coordinated program. Meters that conform to this standard have firmware that can be securely upgraded, providing an ability to deploy changes to meter firmware to address issues uncovered by testing or expected revisions to the metering standards.

*Q1,1b. What is the timeline for initiating a testing and evaluation program for all smart grid technologies for which standards are available?*

*A1,1b.* The identification and development of standards for the Smart Grid is an ongoing process. New use cases and applications for the Smart Grid will continue to grow and evolve over time. As such, the standards supporting these use cases and applications will continue to grow in number and evolve along with test programs supporting these standards. In the Smart Grid environment today very few standards which have been identified up to this point have test programs associated with them. The SGIP Testing and Certification Committee (SGIP TCC) is in the process of creating a Testing and Certification Framework which will identify new required test programs, identify gaps in existing programs and provide best practices to accelerate development of test programs which will help ensure interoperable smart grid products. We expect the SGIP TCC Framework to be completed by the end of the year. In addition, the SGIP TCC will concurrently use this Framework to identify at least two test programs meeting SGIP interoperability requirements. After the validation of this testing Framework, NIST will be in a better position to project the timeline for completion of the development of test programs associated with completed Smart Grid standards. At the beginning of FY 2011 the SGIP TCC will be evaluating the remainder of completed standards on the NIST catalogue of identified standards during FY 2011 to ensure test programs are being developed to ensure Smart Grid interoperability. In our experience with the telecom industry, once a standard is completed, it can take from to 1–3 years to develop a test program to support it depending on the complexity. Our goal is to reduce the test program development cycle time by leveraging the SGIP TCC and its Testing Framework.

## ANSWERS TO POST-HEARING QUESTIONS

*Responses by Mr. John D. McDonald, P.E., Director of Technical Strategy and Policy Development, GE Energy*

**Questions submitted by Chairman David Wu**

*Q1. The NIST FY 2011 budget request includes \$10 million for Standards and Conformity Assessment for Interoperability in Emerging Technologies. This initiative will cover smart grid standards activities, as well as other technologies. What amount of support is sufficient to allow the NIST smart grid standards process to continue at the level needed to develop the standards and the testing requirements? If additional resources were available, what more should be done?*

*A1. The NIST standards effort is vitally important to the successful development and deployment of the smart grid in the U.S. and to ensure harmonized international standards that open global market opportunities for U.S. companies. Much of the funding for the NIST effort was provided through the Recovery Act and those funds will be exhausted in 2011. My understanding is that, apart from the Recovery Act funding, the FY 2011 budget request would, if approved, result in an ongoing NIST smart grid program of \$10 million per year. I would say that \$20–\$25 million per year is the minimum baseline for an effective smart grid standards and measurement program at NIST. The additional funding will be needed to 1) sustain operation of the Smart Grid Interoperability Panel beyond 2011 to carry out the essential work of coordinated standards development; 2) continue development of a comprehensive testing and certification program; and 3) develop new measurement capabilities to ensure robust characterization and control of smart grids.*

## ANSWERS TO POST-HEARING QUESTIONS

*Responses by Mr. Conrad Eustis, Director of Retail Technology Development, Portland General Electric*

**Questions submitted by Chairman David Wu**

*Q1. The NIST FY 2011 budget request includes \$10 million for Standards and Conformity Assessment for Interoperability in Emerging Technologies. This initiative will cover smart grid standards activities, as well as other technologies. What amount of support is sufficient to allow the NIST smart grid standards process to continue at the level needed to develop the standards and the testing requirements? If additional resources were available, what more should be done?*

*A1.* Portland General Electric believes that the NIST budget should be at a maintained at a minimum of \$10 million per year, and if possible increased for the next two years. The work of standards development and testing consists of three primary activities.

1. Initiative Management, Governance and Communications
2. Standards Development where gaps exist, the work of the Priority Action Plan (PAP) groups
3. Interoperability Testing including development tools, testing and audits

The current \$10 million budget is being consumed on mostly the first two items; these efforts have established processes but it should be noted that these processes rely heavily on volunteers to complete important work. The testing process is being developed according to a roadmap under the Smart Grid Testing and Certification Committee. Testing is the most difficult of the processes to be established and implementation will require seed money to create testing tools and set up test labs if required, hence the desire for an increased budget for 2011 and 2012. Unlike the volunteers that write standards documents as time permits, testing requires full time professionals to manage whatever process is established. These resources will be considerably more expensive than the administrative support services that now consume a large part of NIST's budget.

I am not familiar with details of staffing for the PAP groups, but my impression is that the resources are heavily weighted by volunteers; this should be confirmed by NIST. As this new, relatively exciting process wears on, the technical resources required to write competent standards may need to be supplemented by NIST-hired contractors: project managers, systems architects, hardware engineers, software engineers, communication engineers, utility process specialists, etc. These resources would aid the PAP process to drive consensus input to completed quality specifications.

If additional resources are available they should be used to proactively seek input from utilities and their vendors with a focus on what should be done to aid standards adoption by these groups. Collecting input from each group is an independent effort. Portland General Electric's written testimony elaborates on why this is such an important task.

## Appendix 2:

---

ADDITIONAL MATERIAL FOR THE RECORD

*Responses by Dr. George W. Arnold, National Coordinator for Smart Grid, National Institute of Standards and Technology*

**Verbal Questions from Subcommittee by Chairman David Wu**  
***(Verbal questions within the unedited written transcript)***

*Q1. No, the question is whether the privacy groups were an outlier and you reached out to a bunch of other folks and not them?*

A1. NIST has recognized the importance of privacy issues for the Smart Grid from the beginning of NIST's efforts under EISA 2007. In 2009, NIST proactively included a working group focused on privacy as part of the initial establishment of its Cyber Security Coordination Task Group, which has since become the privacy subgroup of the Cyber Security Working Group of the Smart Grid Interoperability Panel. NIST has primarily relied on weekly teleconferences, regular conferences, face-to-face meetings and additional peer-to-peer outreach within the cyber security and privacy communities to inform and learn from interested parties about its Cyber Security Working Group and task groups. In addition, NIST initiated outreach efforts to inform a broader community about NIST Smart Grid activities through multiple Federal Register Notices asking for public review and comments on the NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, and two drafts of NIST Interagency Report 7628 (Smart Grid Cyber Security Strategy and Requirements, now titled Guidelines for Smart Grid Cyber Security). This outreach, particularly outreach through the Federal Register Notices, has been successful in encouraging privacy advocates and others to participate in the NIST process. For example, there are several privacy advocacy groups that participate in our privacy subgroup, including EPIC, Center for Democracy and Technology (CDT), Future of Privacy Forum, and the Electronic Frontier Foundation (EFF). The NIST Smart Grid Interoperability Panel is also working to identify and engage additional groups for outreach, including for example venture capital firms, state and local regulators, consumer groups and other sections of the broad Smart Grid community.

*Q2. What resources do you think NIST will need to appropriately develop standards at a pace which I think the industry and our Nation needs? And if additional resources were appropriated by this Congress, what additional activities or what delta and speed could you achieve?*

A2. NIST is fortunate to have received ARRA funding (\$17 million, consisting of \$12 million from DOE and \$5 million from NIST's own ARRA appropriation) to start the external NIST Smart Grid program by contracting with an administrator to support NIST in establishing the Smart Grid Interoperability Panel. This funding has also permitted additional contracted technical support to help NIST address a selected set of high priority action plans to fill identified standards gaps. In addition, NIST has received \$5 million in the FY 2010 enacted appropriation to support a new Smart Grid Interoperability initiative. Collectively, these resources have enabled NIST to effectively carry out its program to date with successes as noted in George Arnold's written testimony. Current ARRA funding will be expended in FY 2011. An additional initiative to support Smart Grid Interoperability is proposed as part of the President's Budget for FY 2011 in order to sustain the NIST program. Any additional resources would be used to accelerate the development and implementation of a testing and certification framework to support Smart Grid interoperability and cyber security, to accelerate standards development to fill gaps that have been identified, and to develop a comprehensive measurements research program to better characterize and monitor the system-level performance and stability of the Smart Grid. This work would be conducted through NIST's internal efforts and the efforts of external contracted organizations including standards and testing/certification groups.

*Q3. Is there anything we can do at the international standards-setting level or with other mechanisms available to us to provide both carrots and sticks for international cooperation and harmonization or standards?*

A3. NIST is actively engaged in and is providing leadership in all the international standards bodies relevant to the Smart Grid. In addition, NIST has bilateral engagements with counterparts in many other countries, including Canada, Mexico, Brazil, Japan, Korea, China, India, Singapore, Australia, the EU and member states, and Israel. NIST is also working closely with DOE in partnering with other major economies to establish a the International Smart Grid Action Network to provide a multilateral forum for coordination. As indicated in the written testimony,

China's standardization activities in the Smart Grid present a concern because of China's preference for indigenous innovation and the fact that we have limited visibility into China's domestic standardization activities relating to the Smart Grid. NIST has initiated a dialog with State Grid Corporation of China to explore opportunities for collaboration through participation in standards development organizations such as the International Electrotechnical Commission and through the NIST coordinated Smart Grid Interoperability Panel. Specifically, NIST is supporting the work of several working groups within the International Electrotechnical Commission (IEC), especially Technical Committee 57, that are harmonizing the IEC standards with others. These working groups, which include representatives from China as participating members, are revising standards to be harmonized with others, such as IEEE standards, as identified by NIST in Priority Action Plans as part of the NIST Framework and Roadmap for Smart Grid Interoperability Standards.

NIST is also exploring means to build upon its existing collaborations with key Chinese entities such as the Standardization Administration of China (SAC), the Certification and Accreditation Administration of China (CNCA), the China National Institute for Standardization (CNIS) and the China Electronics Standardization Institute (CESI) for engagement in the international standards development for Smart Grid standardization. In specific areas such as standards to support fast charging for electric vehicles, NIST has taken a more active role (in coordination with others in the Federal Government, including the Department of Energy) in outreach to Chinese entities to address specific issues.

The most effective way for Congress to provide "carrots and sticks" to encourage international cooperation and harmonization of standards is by continuing to provide clear policy that standards for the Smart Grid in the U.S. will be based on the standards identified by NIST. This policy was enacted through the provisions in EISA directing FERC to adopt standards based on NIST-identified standards, and establishing use of NIST-identified standards a criteria for DOE Smart Grid grants. Since NIST is basing its framework upon international standards wherever possible—nearly 80% of the standards included in the Release 1.0 framework are produced by international SDOs—this is encouraging other countries to cooperate with NIST in creating global standards so that they can access the U.S. market and U.S. companies can access international markets.