Testimony of

Cita M. Furlani
Director
Information Technology Laboratory

National Institute of Standards and Technology
United States Department of Commerce

Before the
House Committee on Homeland Security
Subcommittee on Emerging Threats, Cybersecurity, and
Science and Technology
United States House of Representatives

July 21, 2009

Introduction

Madam Chair Clarke, Ranking Member Lungren, and Members of the Subcommittee, I am Cita Furlani, the Director of the Information Technology Laboratory 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 role in ensuring the cyber security and reliability of the information and communication aspects of the Smart Grid as well as its physical security.

As the Nation's measurement and standards institute, NIST has earned a reputation as an impartial, technically knowledgeable third party with a long history of working collaboratively with industry and other government agencies. These strengths allow NIST to make a unique contribution to the establishment of the Smart Grid.

Recognizing the benefit of focusing NIST's technical expertise and industry-oriented mission on what is one of the Nation's most pressing issues, Congress, in the Energy Independence and Security Act of 2007 (EISA) called on NIST to take a leadership role in ensuring an interoperable, secure, and open energy infrastructure that will enable all electric resources, including demand-side resources, to contribute to an efficient, reliable electricity network. Specifically, EISA gave NIST "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…" Cyber security and associated standards are being addressed as part of this Smart Grid Interoperability Framework that is under development.

NIST's three-phase approach is to:

- Build on the relationship with the Department of Energy (DOE), Federal Energy Regulatory Commission (FERC), the Department of Homeland Security (DHS), and other federal stakeholders to further engage utilities, equipment suppliers, consumers, standards developers and other stakeholders to achieve consensus on Smart Grid standards. By early fall, the process will deliver:
    - the Smart Grid architecture framework;
    - priorities for interoperability and cybersecurity standards, and an initial set of standards to support implementation; and
    - plans to meet remaining standards needs.
- Launch a formal public-private partnership to facilitate development of additional standards to address remaining gaps and integrate new technologies.
- Develop a plan for testing and certification to ensure that Smart Grid equipment and systems conform to standards for security and interoperability.

After issuing the initial set of priorities, standards and action plans in early fall, NIST will initiate the partnership and complete a testing-and-certification plan by the end of the year.

NIST views its role as accelerating the process by which the standards development can occur. NIST plans to implement the above mentioned public-private partnership to serve as a mechanism to organize stakeholders and drive priority-setting of the standards. The actual standards development work is a process that takes place largely in the private sector, with standards development organizations, utilities, and other stakeholders. The duration of those processes will depend on the complexity of the specific problem. In some cases, it will occur very quickly -- months -- and in other cases, if it's technically very challenging, it may take considerably longer. But in the case of Smart Grid, NIST is moving as expeditiously as possible to get the framework set and move the standards development process along.

NIST is reaching out to the private sector and is using our expertise to identify where the barriers exist, where relevant standards currently exist, where standards exist but are not interoperable, and where gaps exist that require standards to be developed. With appropriations from the American Recovery and Reinvestment Act (PL 111-05), NIST is significantly expanding the public-private coordination so we can move more rapidly to make needed progress in Smart Grid interoperability standards. We are working closely at the interagency level to develop the detailed actions to support this expanded effort. This will allow us to define the interoperability framework (system architecture); establish standards development priorities; support standards assessments; identify standards and conformity testing gaps; and accelerate standards development and harmonization efforts to provide the secure and reliable interchange of information that is necessary to accomplish the Smart Grid mission.

NIST will use the EPRI report in drafting the NIST Smart Grid Interoperability Standards Framework. The NIST document will describe a high-level architecture, identify an initial set of key standards, and provide a roadmap for developing new or revised standards needed to realize the Smart Grid. The first release of the NIST-prepared framework is planned to be available in September. In a *Federal Register* notice published on June 9, NIST released for public comment an *Initial List of Smart Grid Interoperability Standards.* This preliminary set of standards and specifications is identified for inclusion in the Smart Grid Interoperability Standards Framework, Release 1.0, and additional standards and specifications are anticipated to be included based on analyses of workshop input and public comments.

An initial step in this process is the release of a draft report, *Report to NIST on the Smart Grid Interoperability Standards Roadmap,* that identifies issues and priorities for developing interoperability standards for the Smart Grid. In a *Federal Register* notice published on June 30, 2009, NIST formally announced the availability for public comment of this nearly 300-page report, prepared under contract by the Electric Power Research Institute (EPRI).

I would like to caution, however, that the process of creating comprehensive and effective standards can be time-consuming and difficult. To be effective, standards must be developed with broad representation and buy-in from all key stakeholders. It can take

time to do this right, but NIST is establishing an agile framework that will meet the urgent national need for specific Smart Grid standards. The proposed approach will provide that type of expert input through a voluntary consensus standards development process, while maintaining the aggressive schedule needed to develop the Smart Grid.

Understanding the Risk

For the reliability of the electric power industry to be fully realized, cyber security and physical security concerns must be addressed in addition to assuring interoperability. Congress recognized this in specifically calling out the issue of cyber security in the EISA legislation. This is a critical issue due to the increasing potential of cyber attacks and incidents against this critical sector as it becomes more and more interconnected. Existing vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways.

Additional risks to the grid include:

- Increasing the complexity of the grid that could introduce vulnerabilities and disruptions and increase exposure to potential malicious attackers and unintentional errors;
- Linked networks can introduce common vulnerabilities;
- Increasing vulnerabilities to communication and software disruptions that could result in denial of service or compromise the integrity of software and systems;
- Increased number of entry points and paths for potential adversaries to exploit;
- Potential for compromise of data confidentiality, including the breach of customer privacy; and
- Increasing vulnerabilities to potential physical attacks or disruptions, such as those due to Electromagnetic Pulse (EMP), Electromagnetic Interference (EMI), and Geomagnetically Induced Currents (GICs).

The need to address potential vulnerabilities has been acknowledged across the Federal government including by NIST, DHS, DOE and FERC. This need has also been cited in the 60 Day Cyberspace Policy Review, which states that "…as the United States deploys new Smart Grid technology, the Federal government must ensure that security standards are developed and adopted to avoid creating unexpected opportunities for adversaries to penetrate these systems or conduct large-scale attacks." With the adoption and implementation of the Smart Grid, the IT and telecommunication sectors will be more directly involved. These sectors have existing cyber security standards to address vulnerabilities, conformity assessment programs to evaluate cyber security products, and assessment programs to identify known vulnerabilities in systems. These vulnerabilities need to be assessed in the context of the Smart Grid.

Another issue for the Smart Grid and the implementation of cyber security standards is the concern that legacy equipment may be difficult to modify to meet the new standards

developed. The issue of legacy equipment is not unique to the Smart Grid. There are many industrial control systems and IT systems that do not employ the most current suite of cyber security controls. In addition, the life cycle for information technology, particularly for software is very short – as short as six months for many applications -- and the knowledge and skill level of adversaries to attack these systems continues to increase. To address this issue, the Smart Grid cyber security strategy must address the addition and continual upgrade of cyber security controls and countermeasures to meet increasing threats. These new controls and countermeasures may be allocated to stand-alone components within the overall Smart Grid architecture.

The overall cyber security strategy for the Smart Grid must examine both domain-specific and common requirements when developing a mitigation strategy to ensure interoperability of solutions across different parts of the infrastructure. The following is a preliminary list of cyber security requirements applicable to the Smart Grid as a whole:

- Identification and authentication to components of the grid to system entities;
- Physical and logical access control to protect critical information;
- Integrity to ensure that modification of data or commands is detected;
- Confidentiality to protect sensitive information, including Personally Identifiable Information (PII) and proprietary information;
- Availability to ensure that intentional attacks, unintentional events, and natural disasters do not disrupt the entire Smart Grid or result in cascading effects;
- Techniques and technologies for isolating and repairing compromised components of the Smart Grid;
- Auditing to monitor changes in the Smart Grid; and
- Supply chain security to ensure that products and services are not compromised at any point in the life cycle, a defense-in-breadth strategy; and
- Availability to ensure that intentional attacks, whether physical or cyber, unintentional events, and natural disasters do not disrupt the entire Smart Grid or result in cascading effects.

The cyber security strategy will require the development of an overall cyber security architecture to address potential single points of failure, conformity assessment procedures for Smart Grid devices and systems, and certification criteria for personnel and processes.

The Cyber Security Standards Landscape

In addition to understanding and assessing the risks related to the Smart Grid's information and communications networks, it is important to gauge the applicability of existing and new cyber security standards to the Smart Grid. Several standards activities are ongoing including:

- The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Cyber Security Standards CIP-002 through CIP-009, which provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Power System;

- The International Society for Automation (ISA)-99/International Electrotechnical Commission (IEC) 62443 suite of standards that address Security for Industrial Control Systems;

- The Advanced Metering Infrastructure Security task force (AMI-SEC), formed to define common requirements and produce standardized specifications for securing AMI system elements. These requirements are for electric utilities, vendors, and stakeholders; and

- NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems. This SP provides guidance for Federal agencies on cyber security controls with one section of the SP specifically addressing industrial control systems.

Although these standards are being developed by different standards bodies, there is significant interaction among the working groups. For example, there are current efforts to harmonize the NERC CIP, ISA99/IEC 62443, and NIST SP 800-53.

Standards are being assessed for applicability and interoperability across the domains of the Smart Grid, rather than developing a single set of cyber security requirements applicable to all elements of the Smart Grid. That is, the cyber security requirements of different domains, such as home-to-grid and transmission and distribution, may not be the same. For example, there are significant cyber security requirements to ensure the confidentiality of Personally Identifiable Information (PII) in the home-to-grid domain that may not be required at the transmission and distribution domain.

To achieve secure interoperability, products and systems will require conformity assessment that can be developed by NIST. Conformity assessment verifies that products adhere to the specifications defined in the standards. Once a standard has been published, conformity assessment can accelerate product development by giving vendors well-defined criteria to meet. Such testing should ensure that cyber security standards are effective and do not adversely impact interoperability.

Community Partnership

NIST is working with the International Society of Automation (ISA), the International Electrotechnical Commission (IEC), and the North American Electric Reliability Corporation (NERC) on current cyber security standards. NIST also works with other standards bodies, such as ISO, IEEE, and Internet Engineering Task Force (IETF) on

cyber security standards. We will continue to coordinate with all these standards bodies in the development/revision of cyber security standards applicable to the Smart Grid.

To help ensure that we are addressing the cyber security requirements of the Smart Grid as part of the NIST Smart Grid Interoperability Framework, NIST has established a Cyber Security Coordination Task Group (CSCTG), including members from the Domain Expert Working Groups (DEWG) as well as cyber security and control systems experts from academia and the IT and telecommunications communities. The DEWGs are groups of technical experts established by NIST and the GridWise Architecture Council (GWAC) for information sharing on Smart Grid standards and interoperability issues in identified Smart Grid domains: transmission and distribution, home-to-grid, business-to-grid, and industry-to-grid.

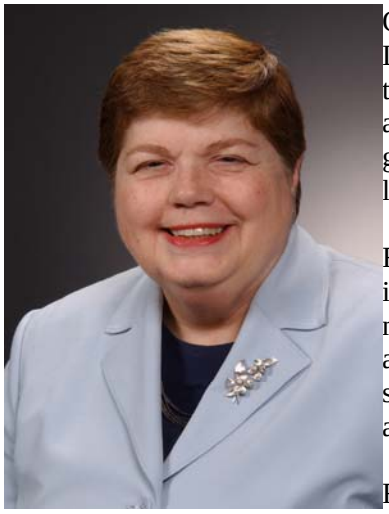
The CSCTG will coordinate among the DEWGs so that cyber security is addressed consistently and comprehensively in the DEWG discussions and work products. The focus of the CSCTG is to leverage the expertise of the members to identify the overall threats, vulnerabilities and risks to the proposed Smart Grid. In addition to cyber security, some physical security issues, including threat assessments related to electromagnetic pulse (EMP), electromagnetic interference (EMI) and geomagnetically induced currents (GIC), related to threat assessments, are also being considered within the CSCTG. This information will be used to identify the appropriate cyber security controls that will be allocated to various domains of the Smart Grid. The CSCTG is also considering a layered approach to cyber security to ensure that if one level is compromised, the next layer remains secure - a defense-in-depth strategy. These cyber security controls will be assessed by CSCTG members for effectiveness, scalability, and impacts on cost and the reliability of the Smart Grid, and will be integrated into the Smart Grid architecture from initiation. Interest is significant, and over 150 individuals have joined the CSCTG to date.

NIST will also coordinate closely with DOE, DHS, and FERC in the development of all smart grid cyber security products, and is also working closely with DOE, FCC and others to examine potential Smart Grid electromagnetic interference issues.

Conclusion

NIST is proud to have been given such an important role in Smart Grid cyber security through the EISA legislation. We believe that with the continued cooperation and collective expertise of the industry in this effort, we will be able to establish the cyber security standards, within the interoperability and standards framework, to ensure that the Smart Grid vision becomes a reality.

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



Cita M. Furlani is Director of the Information Technology Laboratory (ITL). ITL is one of nine research Laboratories within the National Institute of Standards and Technology (NIST) with an annual budget of $85 million, 335 employees, and about 150 guest researchers from industry, universities, and foreign laboratories.

Furlani oversees a research program designed to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology through research and development in information technology, mathematics, and statistics. Through its efforts, ITL seeks to enhance productivity and public safety, facilitate trade, and improve the quality of life.

Furlani has several leadership responsibilities in addition to those at NIST. Currently, she is Co-Chair of the Interagency Working Group on Digital Data, Co-Chair of the Subcommittee on Quantum Information Science, and Co-Chair for Strategic Planning for the Subcommittee on Networking and Information Technology Research and Development, all under the auspices of the National Science and Technology Council. She also serves as Co-Chair of the Technology Infrastructure Subcommittee of the Interagency CIO Council.

Furlani has served as the Chief Information Officer (CIO) for NIST. As CIO, Furlani was the principal adviser to the NIST Director on the planning, execution, evaluation, and delivery of information technology services and support.

Furlani also served as director of the National Coordination Office for Networking and Information Technology Research and Development. This office, reporting to the White House through the Office of Science and Technology Policy and the National Science and Technology Council, coordinates the planning, budget, and assessment activities for the 12-agency Networking and Information Technology R&D Program.

Previously, Furlani was Director of the Information Technology and Electronics Office within the Advanced Technology Program (ATP) at NIST. Before joining ATP, Furlani served as Chief of the Office of Enterprise Integration, ITL, NIST, coordinating Department of Commerce activities in the area of enterprise integration. Furlani also served as special assistant to the NIST Director in the Director's role as Chair of the Committee on Applications and Technology of the Administration's Information Infrastructure Task Force. Previously, Furlani was on detail as technical staff to the Director of NIST in the position of Senior Program Analyst. Prior to August 1992, she managed research and development programs within the NIST Manufacturing Engineering Laboratory, applying information technology to manufacturing since1981.

She earned a Master of Science degree in electronics and computer engineering from George Mason University and a Bachelor of Arts degree in physics and mathematics from Texas Christian University. She was awarded two Department of Commerce Bronze Medal Awards in 1985 and 1993 and the Department of Commerce Silver Medal Award, in 1995.