Testimony of
Patrick D. Gallagher, Ph.D.
Deputy Director

National Institute of Standards and Technology
United States Department of Commerce

Before the
Committee on Energy and Natural Resources
United States Senate

March 3, 2009

Chairman Bingaman, Ranking Member Murkowski and Members of the Committee, thank you for the opportunity to appear before you today to discuss the National Institute of Standards and Technology's (NIST's) role to enable a resilient Smart Grid composed of secure and interoperable devices and systems. NIST carries out this work in coordination with the Department of Energy (DOE) and the Federal Energy Regulatory Commission (FERC), both represented here today.

The availability of clean, reliable and affordable energy is essential to the economic welfare and security of our Nation. We can improve our energy supply through increased use of new renewable and distributed energy sources provided that we can make them widely accessible to industry, businesses and consumers through the Nation's electric power grid. This, however, is not an easy task given the current state of the electric power grid.

As stated by President Obama, we need to "update the way we get our electricity by starting to build a new Smart Grid that will save us money, protect our power sources from blackout or attack, and deliver clean, alternative forms of energy to every corner of our nation."[1]

For this vision to succeed, utilities and others who are implementing the Smart Grid need to be able to purchase equipment in the marketplace and readily incorporate it into the Smart Grid so that it works seamlessly and interoperates with all other systems.

Interoperability refers to the ability of a system or a product to work with other systems or products without special effort on the part of the customer. Achieving interoperability requires reliable standards and validated performance – that is the challenge for NIST.

Under the Energy Independence and Security Act (EISA) of 2007 (Title XIII, Section 1305), NIST has "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…" The American Recovery and Reinvestment Act provided $10 million for NIST for this purpose.

NIST is well-suited for this role. The agency has a reputation as an impartial, technically knowledgeable third party with a long history of working collaboratively with industry and other government agencies, including DOE and now the Federal Energy Regulatory Commission (FERC). NIST also has provided measurement technology and assistance to utilities, equipment manufacturers, and other power-system stakeholders. Only through collaborative efforts with all stakeholders will Smart Grid solutions to the complex and layered problems of interoperability be adopted by the many participants – power generators, Independent System Operators (ISOs), Regional Transmission Operators (RTOs), electric service providers, consumers, vendors, etc

[1] Gross, Grant. "Obama Includes Broadband, Smart Grids in Stimulus Package." Stimulus Speech. January 8, 2009. IDG News Service. www.itworld.com/government.

The present electric power grid infrastructure is based on numerous standards, and many organizations are now assessing their applicability to the Smart Grid and determining what new standards need to be developed. NIST is working with these organizations to "tie it all together" so that unnecessary redundancy, conflicts, and gaps among the standards can be avoided and resolved. For there to be true interoperability, new Smart Grid devices also require testing to show that they conform with the standards.

The nation's electrical grid has been called "the greatest engineering achievement of the 20th century" and "largest interconnected machine on Earth." Due to the complexity of the grid, we and many others believe that there can be no single standard for Smart Grid devices and systems. Rather, we expect suites of standards to be developed for different aspects, including distributed energy resources (DER), demand response (DR) devices/appliances, electric vehicles, wide area measurement systems (WAMs), and other parts of the Smart Grid vision. The Smart Grid also needs to be evolutionary – beginning with the existing energy infrastructure and evolving as new innovations arise and the energy infrastructure and consumer needs and behavior change. This means that standards, conformance tests and other efforts to ensure interoperability must also continue to evolve.

NIST has begun the coordinating of the interoperability framework by bringing together the many stakeholders. Working in close cooperation with the DOE and its Grid Wise Architecture Council (GWAC), domain expert working groups have been established that cover key areas of the Smart Grid, including transmission & distribution, and commercial, industrial, and residential buildings. Additional groups and task forces to address higher-level and crosscutting issues – in business and policy, cyber security, and smart grid framework/architecture, to name a few – have been initiated.

Our goal is to bring these experts together, many of whom have not worked in close coordination before, to promote the information sharing necessary for the development of effective Smart Grid standards. We are using their expertise to support the framework development by identifying where the barriers to interoperability exist. In addition, we are identifying where relevant standards currently exist, where standards exist but are not interoperable, and where gaps exist that will need to be filled by new standards.

With appropriations from the recent enactment of the American Recovery and Reinvestment Act (ARRA), NIST will make significant headway working with its team comprising of NIST staff, contractors, and staff from the Department of Energy (DOE), the Federal Energy Regulatory Commission (FERC), the Grid Wise Architecture Council (GWAC) and many other industry and standards developing organizations to more rapidly make progress in the following ways:

- **Interoperability Framework/Architecture**. An initial version of the interoperability framework will be developed– one that will have the flexibility to evolve as the Smart Grid develops.

- **Smart Grid Standards Gap Analysis and Roadmap**. We will develop a smart grid standards gap analysis and road map to identify critical areas and guide interoperable standards development.
- **Publicly Accessible Interoperability Knowledge Base.** NIST plans to create a publicly-accessible interoperability knowledge base that will be the repository of the information necessary to perform standards assessments.
- **Accelerate Standards Development.** With the clear picture of the standards landscape and roadmap established, NIST will work effectively with standards development organizations (SDOs), contractors, and industry experts and other stakeholders to accelerate the development of scalable, compatible and interoperable standards.

I would like to caution, however, that the process of creating good consensus-based standards is not easy. To develop robust standards and ensure their use, the standards developing groups should have broad representation from all key stakeholders. Achieving consensus agreement among such a diverse group of stakeholders can take significant time, particularly if the resulting standards need to be applicable domestically and internationally.

Having good standards alone does not guarantee interoperability. Conformity assessment testing is necessary to ensure that the Smart Grid devices and systems developed based on the standards are truly interoperable. The NIST laboratories have long supported the development of the reference implementations of the standards for emerging technologies and the tests that will validate their interoperability.

NIST has been providing technical support for the development of Smart Grid devices for several years now. These include the Phasor Measurement Units, devices that will enable operators to get the information about grid conditions that they need to limit the effects of disruptions and instabilities in the grid and avoid large scale blackouts as occurred in the Northeast in August 2003. They also include high-megawatt power converters that will provide the flexibility to readily and reliably connect alternative and renewable resources to the grid.

Under the EISA, once sufficient consensus has been achieved, FERC will begin the rulemaking process for adopting standards and protocols. NIST's goal is to support this action by working closely with stakeholders to identify and develop the standards as quickly as possible based on broad participation and expert input. NIST believes that the most effective standards will be developed through broad input from experts, including industry and other stakeholders. The proposed approach will provide expert input through a voluntary consensus standards development process, while pursuing the aggressive schedule needed to develop the Smart Grid.

Finally, NIST has the important responsibility to develop Federal Cyber Security standards. Interoperability across the electric power grid infrastructure will do us no good if the grid is disabled by a cyber attack enabled by access through the Smart Grid system. Security must be integrated into the interoperability framework in order to ensure

the integrity and availability of the infrastructure and the privacy of Smart Grid users. The cyber security strategy for the Smart Grid must account for both domain-specific and common risks when developing interoperability solutions. Collaborative efforts will enable the development of the standards needed to reach our vision for Smart Grid interoperability.

The following is a preliminary list of cross cutting security requirements for the Smart Grid that have been identified and will be addressed by NIST and its team:

- *Identification and authentication* to provide unambiguous reference to system entities.
- *Access control* to protect critical information.
- *Integrity* to ensure that the modification of data or commands is detected.
- *Confidentiality* to protect sensitive information, including personally identifiable information (PII) and business identifiable information (BII).
- *Availability* to ensure that intentional attacks, unintentional events, and natural disasters do not disrupt the entire Smart Grid or result in cascading effects.
- *Security architecture* to ensure that there is no single point of failure.
- *Conformity Assessment Procedures* for Smart Grid devices and certification criteria for the personnel and processes.
- *Strategies for isolating* and repairing compromised components of the Smart Grid.
- *Auditing* to monitor changes to the Smart Grid.
- *Supply chain security* to ensure that products and services are not compromised at any point in the life cycle. This is a defense-in-breadth strategy.

NIST is proud to have been given such an important role in the EISA legislation. We have received enthusiastic support from DOE, GWAC, and many industry and other stakeholders. We believe that with the continued cooperation and collective expertise of the industry in this effort, we will be able to establish the interoperability and standards frameworks that will enable the Smart Grid vision to become a reality.

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

**Dr. Patrick D. Gallagher, Deputy Director**

Dr. Patrick Gallagher is the Deputy Director of the U.S. Department of Commerce's National Institute of Standards and Technology (NIST). He is also carrying out the responsibilities of the Director. (The NIST Director position is vacant.) Gallagher provides high-level oversight and direction for NIST. The agency promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology. NIST's FY 2008 resources total $931.5 million and the agency employs about 2,900 scientists, engineers, technicians, support staff and administrative personnel at two main locations in Gaithersburg, MD, and Boulder, CO.

Prior to becoming Deputy Director, Gallagher served as Director of the NIST Center for Neutron Research (NCNR), a national user facility for neutron scattering on the NIST Gaithersburg campus, since 2004. The NCNR provides a broad range of neutron diffraction and spectroscopy capability with thermal and cold neutron beams and is presently the nation's most used facility of this type. Gallagher received his Ph.D. in Physics at the University of Pittsburgh in 1991. His research interests include neutron and X-ray instrumentation and studies of soft condensed matter systems such as liquids, polymers and gels. In 2000, Gallagher was a NIST agency representative at the National Science and Technology Council (NSTC). He has been active in the area of U.S. policy for scientific user facilities and was chair of the Interagency Working Group on neutron and light source facilities under the Office of Science and Technology Policy.