Questions for Patrick Gallagher
National Institute of Standards and Technology
Committee on Energy and Natural Resources Hearing- March 03, 2009

Questions from Senator Bingaman:

(1) One of the often stated key benefits of Smart Grid is in its ability to integrate large quantities of intermittent renewable resources into the grid and to efficiently route this power where it is needed. To achieve this will clearly require both the build-out of new transmission to renewable resource rich locations as well as upgrading our current grid to have the intelligence to handle these intermittent resources.

In order to achieve the benefits that we want from Smart Grid, how much new transmission do you foresee being needed? And how do we prioritize the building of new transmission vs. upgrading our current grid?

Answer: NIST will defer to DOE and FERC on estimating "how much new transmission" is needed. However, it is clear that there is a need to build out new transmission to renewable resource-rich locations and to upgrade the grid to better handle these resources if our nation is to fully realize the benefits of Smart Grid. In addition, better and more storage and power conversion technologies are needed to make best use of these large-scale intermittent resources. NIST is working to develop the interoperability framework to coordinate and prioritize standards development to ensure that the Smart Grid devices and systems that will accommodate these large renewable power sources will be interoperable, and beyond that, allow for and encourage customers to adjust their energy usage.

(2) "Smart Metering" projects for residential consumers have become the poster child of the Smart Grid. However, some studies have found that the majority of the benefits of the Smart Grid will result from investments in grid transmission and distribution system upgrades and optimization, with only a small percentage of energy savings and emission reductions coming from smart metering programs. Could you comment on this? And how should we take these findings into consideration when prioritizing which Smart Grid demonstration projects to fund?

> *NOTE: as a data point, the Climate Group SMART 2020 Report estimates that 85% of the carbon reduction benefits of a Smart Grid come from Grid Optimization and Renewables Integration, and only 15% will come from End-User Energy Management.*

Answer: The Smart Grid addresses several goals, each of which is important. Renewable energy generation leads to the greatest impact for carbon reduction, and efficiency improvements in transmission and distribution lead to less wasted energy and greater reliability. Smart Metering addresses a different goal, reducing energy use by customers and smoothing load shape to increase grid utilization. Demonstration projects are

needed in each of these areas to inform and validate the selection of standards needed for broad deployment of Smart Grid technologies. Testing and validating Smart Grid standards interoperability is a key aspect of NIST's program. We are working closely with DOE, and anticipate testing and validation will be a key aspect as the Smart Grid standards move forward.

(3) After the Department of Energy has spent out its nearly $4.5 Billion on Smart Grid Investments, how do we measure whether that money has been spent effectively? How soon and what improvements in our grid should we expect to see?

Answer: The Department of Energy has a clear vision of what Smart Grid success looks like and will set metrics to assess the effectiveness of its investments. Deployment of some Smart Grid technologies has already begun. For example some major utilities are moving ahead aggressively in deploying technologies such as Smart Metering. The DOE investment will accelerate broad-scale deployment of Smart Grid elements as standards are established, while also supporting demonstration projects to inform standards development and testing of other Smart Grid elements.

(4) Dr. Gallagher, in your testimony you state that NIST, as directed by EISA, will develop suites of standards for different smart grid aspects, including distributed energy resources, demand response devices/appliances, electric vehicles, wide area measurement systems, and other parts of the Smart Grid vision. Furthermore, during the hearing you stated that you expect that by this summer, NIST will have completed a road map to prioritize the order in which smart grid standards need to be developed.

As Senator Bingaman requested in the hearing, please submit to us:

(1) an inventory of the suites of standards to be developed;

(2) Each standard, that to the best of your current knowledge, will need to be developed; and

(3) For each standard, a list of the standards development organizations that would logically be involved in the development of such standard.

Answer: To clarify, I stated at the hearing that NIST would, by this summer, have completed an initial version of a roadmap to prioritize the selection and/or development of standards. The roadmap will include an architecture and framework that will evolve to incorporate new technologies and requirements. Once this initial version of the roadmap is developed, it will be continuously updated and be used as a basis for developing priority actions in support of developing the standards framework.

The appended document lists suites of Smart Grid standards under development in different organizations.

It is important to note that there are several "suites" of standards as well as hundreds of individual standards that are key for Smart Grid interoperability. These suites are in different stages of maturity and cover many Smart Grid devices and functionality. There

are also overlaps among them that require harmonization, some of which are already being addressed.

Some of the existing standards have not yet undergone extensive use and conformity testing that would reveal whether they are truly interoperable, so it is not fully known what the weaknesses are in these standards and where they may need to be modified.

As the roadmap is developed and evolves and as new standards are published, more of these standards issues will be identified and addressed. The attached document lists some of the suites of Smart Grid standards under development in the various Standards Developing Organizations (SDOs). The list is not prioritized, nor is it exhaustive since NIST is continuing to develop the roadmap and standards from other industries such as networking; telecommunications and end use equipment are expected to play key roles in the development of the smart grid infrastructure and input from these industries will be included as the interim roadmap and Smart Grid standards move forward.

Questions around Standards Development for Dr. Gallagher and Ms. Hoffman

(5) Dr. Gallagher, we have heard from many parties, most recently Secretary Chu, that standards and protocols development is lagging behind industry needs, and may soon hinder Smart Grid deployment. While I understand that your agency has lacked appropriated funds up until very recently (when $10 million was appropriated in the American Recovery and Reinvestment Act), how do you plan to ensure that you now will move expeditiously? Can you provide us an approximate timeline for when you expect to begin releasing consensus standards?

Answer: Standards are developed for industry, by industry, through an established consensus process in which government participates. NIST has played an important role, working alongside industry participants, providing both technical expertise and coordination. The recognition of Smart Grid as an urgent national priority, and especially the funding provided by the American Reinvestment and Recovery Act, makes it imperative to develop the standards more rapidly, requiring new approaches. NIST has recently taken several steps to accelerate progress.

We have committed to delivering an interim interoperability standards roadmap by June and are working to expedite this effort using ARRA funding. We are also planning to use the ARRA funding to accelerate the establishment of a public-private partnership, modeled on the most successful elements of the Health Care IT interoperability effort, to select and/or coordinate the development of new standards based on the roadmap. We will focus initially on the selection of existing standards to meet the highest priority needs, while working to develop new or harmonized standards where necessary to meet other needs. We anticipate that initial standards will be selected in 2009.

.

(6) Dr. Gallagher, in your opinion, is it a hindrance to industry and to smart grid development that NIST has not yet begun releasing consensus standards and protocols? At what point would you consider a lack of NIST approved standards a hindrance?

Answer: To clarify, consensus standards in the U.S. are developed by the private sector through standards development organizations (SDOs) and do not normally require formal recognition or approval by NIST. For example, the internet, a network about as complex as the Smart Grid, was established and continues to evolve based entirely on private-sector, voluntary standards. NIST's role is to support this process by working closely with industry and stakeholders as a third party technical expert. NIST and industry believe that this process produces the most effective and widely accepted standards. From that perspective, lack of NIST-approved standards for Smart Grid is not a hindrance to industry.

However, some standards for the Smart Grid may need to be mandated via adoption in regulation to ensure the reliability and security of the Smart Grid, which is one of the nation's critical infrastructures. EISA specifically tasks NIST to coordinate development of an interoperability framework including protocols and model standards, which is appropriate for this reason. The steps NIST is taking will accelerate the availability of NIST-approved standards to support regulation so that they do not become a hindrance to industry.

Questions from Senator Murkowski:

(1)What does Smart Grid technology promise in terms of reliability? A smarter grid is supposed to enhance our system's security but technologies like smart meters, sensors and advanced communications networks can actually increase the vulnerability of the grid to cyber attacks.

Answer: An important component of reliability for the electric industry is cyber security. This includes addressing cyber security incidents. Currently, many components of the grid are interconnected to the Internet, either directly, or via the business component of a company. This has increased the potential for cyber attacks that could compromise the availability and/or integrity of the existing grid. This requirement to address potential vulnerabilities has been acknowledged by the Department of Homeland Security (DHS), through the Critical Infrastructure Protection (CIP) Program. They have a vulnerability assessment program that is available to critical infrastructures. Also, DHS is working with the critical infrastructures to promote reporting of potential incidents through the US – Computer Emergency Readiness Team (US-CERT) program. In addition, there are several current initiatives to develop cyber security standards for components of the existing grid. These standards are intended to address existing vulnerabilities. Finally, the IT and telecom sectors have cyber security standards to address vulnerabilities, conformity assessment programs to evaluate cyber security products, and assessment programs to identify known vulnerabilities in systems.

► **How do we address these cyber security concerns?**

Answer:

One of the important lessons from the IT and telecom sectors is that network security must be inherently designed into the architecture of the network; it cannot be "bolted on" later. NIST is applying its extensive expertise in both computer security and advanced network technology to systematically assess risk and ascertain security requirements for the Smart Grid architecture.

There are a number of cyber security standards that are being developed that are applicable to the Smart Grid:

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

- The ANSI/ISA-99/IEC 62443 suite of standards for Industrial Automation and Control System Security

- The Advanced Metering Infrastructure (AMI) has formed a Security task force (AMI-SEC) to define common requirements and produce standardized specifications for securing AMI system elements

- NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, which provides security controls for federal agencies, including those who are part of the Bulk Power System (e.g., Tennessee Valley Authority, Bonneville Power Authority). This Special Publication is incorporated by reference in Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements*, making it mandatory for Federal agencies.

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 Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*.

The important objective is to assess the standards for applicability and interoperability across the domains of the Smart Grid, rather than develop a single set of cyber security requirements that is applicable to all elements of the Smart Grid. That is, the cyber security requirements of different domains, such as home-to-grid or transmission and distribution, may not be the same. There are significant cyber security requirements to ensure the confidentiality of Personally Identifiable Information (PII) that may not be required at the transmission and distribution domain.

In addition, the cyber security standards will require conformance testing. Conformance testing verifies that products adhere to the specifications defined in the standards. NIST intends to develop a conformance testing framework for the Smart Grid.

- **Do the agencies have sufficient authority or is additional federal legislation needed?**

Answer: NIST has the necessary authority under the National Technology Transfer and Advancement Act (PL 104-113), the Energy Independence and Security Act (EISA), and other legislation, to carry out its role to coordinate the development of an interoperability framework for the Smart Grid.

(2) The Stimulus bill provided an unprecedented $4.5 billion in federal funds for smart grid activities. In your opinion, what is the best way to allocate these funds – matching grants for technology investments; research and development; pilot programs? Over what timeframe? What are the necessary first steps?

Answer: The Department of Energy (DOE) has the responsibility of allocating the $4.5 billion in funds, and DOE is best able to provide answers to these questions. NIST believes that there is great benefit to ensuring that funded demonstration projects support and inform the standards development process and validate selected standards by confirming interoperability under realistic operating conditions. In addition, these funds will provide the ability to address important issues to enable the maximum benefit from the Smart Grid investments, including demonstrating the validity of Demand Response benefits, proper operation of dynamic pricing and market/regulations to support that operation, and testing of standards for roadmap interfaces to prove standards and guide conformity testing. NIST believes that widespread dissemination of lessons learned from these demonstration projects, matching grants program and R&D and other activities will support standards development and the creation of future innovation advances.

The Communications Dependency on Electric Power (CDEP) Report, recently approved by the National Communications System (NCS), addresses other salient aspects relating to smart grid technology. For example, recovery transformers and further development of resilient fault-tolerance high voltage lines can well benefit from additional R&D and dedicated deployment funding.

(3) What capabilities and expertise in this area does each of your agencies bring to the table?

Answer: Ensuring interoperability of the Smart Grid requires capabilities in numerous disciplines. NIST brings 1) extensive knowledge of the electric utility industry through its research in supporting measurement technology and testing; 2) expertise in advanced networking technology; 3) expertise in computer and network security; 4) expertise in industrial controls and their interfaces to the electrical infrastructure; 5) expertise in the

technology of buildings and their interfaces to the electric grid; 6) expertise in the consensus standards development process; and 7) expertise in conformity assessment.

(4) What is the role of the Standards Development Organizations (SDOs), such as NEMA, in the NIST framework? When will NIST be ready to utilize the expertise that the SDOs have available?

Answer: SDOs have an essential role in the NIST framework, as standards are developed by SDOs. The large majority of smart grid standards are already under development in an SDO. SDOs bring the stakeholder community together (via company supported volunteers and representatives of other stakeholder groups working in standards committees) to develop standards. NIST is already working with the technical experts who are developing smart grid standards, and already actively engaged with SDOs in developing the smart grid roadmap. NEMA was named in the 2007 EISA for NIST to coordinate with and plays an important role representing a large vendor community. NIST will continue to work with NEMA and other stakeholders to coordinate the development of the interoperability framework.

(5) You testified that there should be no single standard for Smart Grid devices and systems because a smarter grid needs to be evolutionary. How can we best ensure that interoperability standards continue to evolve?

Answer: EISA requires the interoperability framework **"**to be flexible to incorporate regional and organizational differences, and technological innovations." Attributes which will support this goal include, among others, technology neutrality, standards which are performance based rather than design specific, and a layered architecture. The "public-private partnership" entity (referred to in my answer to Senator Bingaman's question) will provide an ongoing mechanism to evolve the interoperability standards.

(6) When will NIST have a Director in place?

Answer: NIST is not aware of any specific timeframe to nominate a new NIST Director.

(7) You caution that it is difficult and time consuming to create good consensus-based standard – particularly if the resulting standards need to be applicable domestically and internationally. Don't standards need to be applied nationwide, in a seamless fashion, or are you suggesting we could consider a more regional approach?

Answer: The standards absolutely need to be applied nationwide to ensure interoperability and they should ultimately be based on international standards. The ability to dynamically move load to match demand and utilize distributed energy sources on a national electrical grid demands a national solution. Furthermore, the interconnection of the US grid with Canada and Mexico requires North American, not just U.S. standards. Finally, the equipment in the network is produced by global

suppliers who want international standards so they can address multiple markets around the world.

Addendum
Smart Grid Families of Standards
(Response to Sen. Bingaman Q#4)

The following list contains leading industry families of standards that will enable the vision of the Smart Grid. The NIST roadmapping process is intended to reveal where in the standards weaknesses, gaps, and overlaps exist and will evolve as new standards are developed and new implementations deployed and tested. The list is not exhaustive since standards from other industries such as networking, telecommunications and end use equipment are expected to play key roles in the development of the smart grid infrastructure.

The families listed below include some standards that are have not yet been completed, released, or published. These families will have to be further developed to ensure that gaps covering additional Smart Grid functions, devices, and systems are addressed. Further analysis is needed to ensure that the standards are harmonized and conformance testing of implementations of these standards is needed to reveal where interoperability issues exist.

International Electrotechnical Commission (IEC) 61968 Family of Standards for Distribution Systems

- IEC 61968-1 (2003-10) Application integration at electric utilities - System interfaces for distribution management - Part 1: Interface architecture and general requirements
- IEC/TS 61968-2 (2003-11) Application integration at electric utilities - System interfaces for distribution management - Part 2: Glossary
- IEC 61968-3 (2004-03) Application integration at electric utilities - System interfaces for distribution management - Part 3: Interface for network operations
- IEC 61968-4 (2007-07) Application integration at electric utilities - System interfaces for distribution management - Part 4: Interfaces for records and asset management
- IEC 61968-14-1: Mapping between MultiSpeak 4.0 and IEC 61968, parts 3 through 10
- IEC 61968-14-2: A CIM profile for MultiSpeak 4.0, one profile for IEC 61968 parts 3 through10

International Electrotechnical Commission (IEC) 61970 Family of Standards for Transmission

- IEC 61970 Energy management system application program interface (EMS-API) - Part 301: Common Information Model (CIM) Base", IEC, Edition 1.0, November 2003
- IEC 61970-1 (2005-12) Energy management system application program interface (EMS-API) - Part 1: Guidelines and general requirements
- IEC/TS 61970-2 (2004-07) Energy management system application program interface (EMS-API) - Part 2: Glossary
- IEC 61970-301 (2005-03) Energy management system application program interface (EMS-API) - Part 301: Common Information Model (CIM) base
- IEC/TS 61970-401 (2005-09) Energy management system application program interface (EMS-API) - Part 401: Component interface specification (CIS) framework
- IEC 61970-404 (2007-08) Energy management system application program interface (EMS-API) - Part 404: High Speed Data Access (HSDA)
- IEC 61970-405 (2007-08) Energy management system application program interface (EMS-API) - Part 405: Generic Eventing and Subscription (GES)
- IEC 61970-407 (2007-08) Energy management system application program interface (EMS-API) - Part 407: Time Series Data Access (TSDA)
- IEC 61970-501 (2006-03) Energy management system application program interface (EMS-API) - Part 501: Common Information Model Resource Description Framework (CIM RDF) schema

American National Standards Institute (ANSI) - C12 Metering Standards

- ANSI C12.19 2008: Utility Industry End Device Data Tables (Revenue Metering) (note: not yet formally released)
- ANSI C12.22 2008: Protocol Specification for Data Communication Networks (note: not yet formally released)

American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE) - BACnet Standard

- ANSI/ASHRAE Standard 135-2004: BACnet--A Data Communication Protocol for Building Automation and Control Networks

International Electrotechnical Commission (IEC) - 61850 Family of Standards for Field Devices

- IEC/TR 61850-1 (2003-04) Communication networks and systems in substations - Part 1: Introduction and overview
- IEC/TS 61850-2 (2003-08) Communication networks and systems in substations - Part 2: Glossary
- IEC 61850-3 (2002-01) Communication networks and systems in substations - Part 3: General requirements
- IEC 61850-4 (2002-01) Communication networks and systems in substations - Part 4: System and project management
- IEC 61850-5 (2003-07) Communication networks and systems in substations - Part 5: Communication requirements for functions and device models
- IEC 61850-6 (2004-03) Communication networks and systems in substations - Part 6: Configuration description language for communication in electrical substations related to IEDs
- IEC 61850-7-1 (2003-07) Communication networks and systems in substations - Part 7-1: Basic communication structure for substation and feeder equipment - Principles and models
- IEC 61850-7-2 (2003-05) Communication networks and systems in substations - Part 7-2: Basic communication structure for substation and feeder equipment - Abstract communication service interface (ACSI)
- IEC 61850-7-3 (2003-05) Communication networks and systems in substations - Part 7-3: Basic communication structure for substation and feeder equipment - Common data classes
- IEC 61850-7-4 (2003-05) Communication networks and systems in substations - Part 7-4: Basic communication structure for substation and feeder equipment - Compatible logical node classes and data classes
- IEC 61850-7-410 (2007-08) Communication networks and systems for power utility automation - Part 7-410: Hydroelectric power plants - Communication for monitoring and control

- IEC 61850-7-420 (2008-02) DER Logical Nodes, Final Draft International Standard (FDIS)
- IEC 61850-8-1 (2004-05) Communication networks and systems in substations - Part 8-1: Specific Communication Service Mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3
- IEC 61850-9-1 (2003-05) Communication networks and systems in substations - Part 9-1: Specific Communication Service Mapping (SCSM) - Sampled values over serial unidirectional multidrop point to point link
- IEC 61850-9-2 (2004-04) Communication networks and systems in substations - Part 9-2: Specific Communication Service Mapping (SCSM) - Sampled values over ISO/IEC 8802-3
- IEC 61850-10 (2005-05) Communication networks and systems in substations - Part 10: Conformance testing

IEEE 1547 Family of Standards for Distributed Energy Resources

- IEEE 1547 Standard for Integrating Distributed Energy Resources within the Electric Power System
- IEEE-P1547.1 standard for interconnection test procedures
- IEEE-P1547.2 guide to 1547 standard
- IEEE-P1547.3 guide for information exchange for DR interconnected with EPS
- IEEE-P1547.4 guide for DR island systems

Zigbee Specification (based on IEEE 802.15.4)

- Zigbee Smart Energy

Cyber Security Standards

Advanced Metering Infrastructure (AMI) System Security Requirements

- ANSI/ISA-99/IEC 62443 suite of standards for Industrial Automation and Control System Security
- FIPS PUB 140-2, Security Requirements for Cryptographic Modules (also ISO ISO/IEC 19790:2006)
- FIPS PUB 180, Secure Hash Standard

- FIPS PUB 186, Digital Signature Standard (DSS)
- FIPS PUB 197, Advanced Encryption Standard (AES)
- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
- IEC/TS 62351-1 (2007-05) Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues
- IEC/TS 62351-2 Power systems management and associated information exchange - Data and communication security - Part 2: Glossary of terms
- IEC/TS 62351-3 (2007-06) Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP
- IEC/TS 62351-4 (2007-06) Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS
- IEC TS 62351-5 Power systems management and associated information exchange - Data and Communication Security - Part 5: Security for IEC 60870-5 and Derivatives
- IEC/TS 62351-6 (2007-06) Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850
- IEC 62443 Industrial communication networks - Network and system security (DRAFT)
    - IEC 62443-1 Terminology, concepts and models
    - IEC 62443-2 Establishing an industrial automation and control system security program
    - IEC 62443-3 Operating a manufacturing and control systems security program
    - IEC 62443-4 Specific security requirements for manufacturing and control systems
    - IEC 62443-5 Security technologies for industrial automation and control systems
- ISA-99: Manufacturing and Control Systems Security
- IEEE P1689 Trial Use Standard for Retrofit Cyber Security of Serial SCADA Links and IED Remote Access
- ISO 27001 information security management system (an ISMS) which replaced the old BS7799-2 standard

- ISO 27002 This is the 27000 series standard number of what was originally the ISO 17799 standard (which itself was formerly known as BS7799-1)

- ISO 27003 guidance for the implementation of an ISMS (IS Management System)

- ISO 27004 information security system management measurement and metrics

- ISO 27005 This is the methodology independent ISO standard for information security risk management

- ISO 27006 guidelines for the accreditation of organizations offering ISMS certification

- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) CIP-001-1 Sabotage Reporting

- NERC CIP-002-1 Critical Cyber Asset Identification

- NERC CIP-003-1 Security Management Controls

- NERC CIP-004-1 Personnel & Training

- NERC CIP-005-1 Electronic Security Perimeter(s)

- NERC CIP-006-1 Physical Security of Critical Cyber Assets

- NERC CIP-007-1 Systems Security Management

- NERC CIP-008-1 Incident Reporting and Response Planning

- NERC CIP-009-1 Recovery Plans for Critical Cyber Assets

- NIST Special Publication (SP) 800-53, *Recommend Security Controls for Federal Information Systems* NIST SP 800-82, DRAFT Guide to Industrial Control Systems (ICS) Security
- The role concept in SCL: 2nd draft, ABB AN-PSTD07002WW, 29 August 2007

International Electrotechnical Commission (IEC) and IEEE Standards Integration for Synchrophasor Measurements

- IEC and IEEE are proposing "Dual Logo" standards development in this area that anticipates integrating related standards from both organizations. These include:

- IEEE C37.118-2005 Standard for Synchrophasors for Power Systems and IEC 61850.

SAE Best Practices and Use Cases for Electric Vehicle Communications

- SAE J2836, Recommended Practice for Communication between Plug-in Vehicles and the Utility Grid (2009 ballot)

- SAE J2847 - Information Report for Use Cases for J2836 (2009 ballot)

Glossary of Smart Grid Private Sector Standards Development Organizations Listed Above

ANSI – The American National Standards Institute

ANSI is a private non-profit organization that oversees the development of voluntary consensus standards for products, services, processes, systems, and personnel in the United States. The organization also coordinates U.S. standards with international standards so that American products can be used worldwide. ANSI accredits standards that are developed by representatives of standards developing organizations, government agencies, consumer groups, companies, and others. These standards ensure that the characteristics and performance of products are consistent, that people use the same definitions and terms, and that products are tested the same way.

ASHRAE –American Society of Heating, Refrigerating, and Air-Conditioning Engineers

ASHRAE is an international technical society for all individuals and organizations interested in heating, ventilation, air-conditioning, and refrigeration (HVAC&R). The Society allows exchange of HVAC&R knowledge and experiences for the benefit of the field's practitioners and the public. ASHRAE provides many opportunities to participate in the development of new knowledge via, for example, research and its many Technical Committees.

IEC – International Electrotechnical Commission

The IEC is a not-for-profit, non-governmental international standards organization that prepares and publishes International Standards for all electrical, electronic and related technologies – collectively known as "electrotechnology". IEC standards cover a vast range of technologies from power generation, transmission and distribution to home appliances and office equipment, semiconductors, fiber optics, batteries, solar energy, nanotechnology and marine energy as well as many others. The IEC also manages three global conformity assessment systems that certify whether equipment, system or components conform to its International Standards.

IEEE – (IEEE does not use a associated name)

IEEE is an international non-profit, professional organization for the advancement of technology related to electricity. It has the most members of any technical professional organization in the world, with more than 365,000 members in around 150 countries.

NERC – North American Electric Reliability Corporation

NERC oversees eight regional reliability entities and encompasses all of the interconnected power systems of the contiguous United States, Canada and a portion of Baja California in Mexico. NERC's major responsibilities include working with all stakeholders to develop standards for power system operation, monitoring and enforcing compliance with those standards, assessing resource adequacy, and providing educational and training resources as part of an accreditation program to ensure power system operators remain qualified and proficient. NERC also investigates and analyzes the causes of significant power system disturbances in order to help prevent future events.

SAE – Society of Automotive Engineers

SAE is a professional organization for mobility engineering professionals in the aerospace, automotive, and commercial vehicle industries. The Society is a standards development organization for the engineering of powered vehicles of all kinds, including cars, trucks, boats, aircraft, and others.