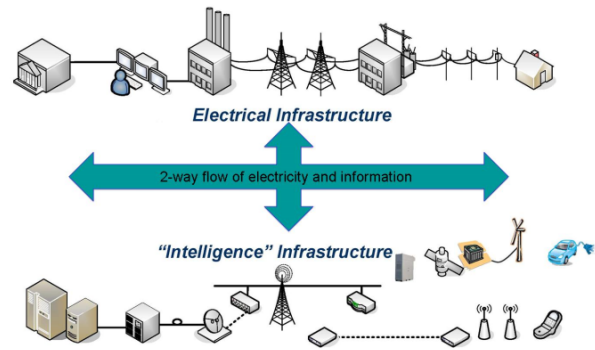


ITL SMART GRID PROGRAM

Under the Energy Independence and Security Act of 2007 (Public Law 110-140, often referred to as “EISA”), NIST has been given “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.” As part of the NIST multidisciplinary team working on electric energy Smart Grid (SG) topics, ITL leads a number of efforts. ITL provides technical expertise as a member of the **Smart Grid Interoperability Panel (SGIP) Smart Grid Architecture Committee** developing the architectural requirements that will be used to guide the development of SG interoperability standards. In addition, ITL provides leadership and expertise to the **SGIP vehicle-to-grid working group’s** efforts to identify and help develop information exchange standards to support the deployment of **electric vehicles**. ITL also supports efforts to characterize performance metrics and develop test methods for the IEEE 1588 standard (IEC 61588) and the complementary power substation profile which can provide critical **timing synchronization** necessary for reliable Smart Grid monitoring and control. Furthermore, ITL applies its technical expertise in the critical areas of Networking and Cybersecurity as described below:

Networking in the Smart Grid

An important part of the Smart Grid is the communications infrastructure used to send command information between generation and distribution systems, and to exchange usage and billing information between utilities and their customers. While there are many possible communications and networking standards that can be used in the context of the Smart Grid, most of these standards were not developed specifically for Smart Grid applications. The critical issues that must be addressed by any communications standard that would be used in the Smart Grid include performance, interoperability, and coexistence. NIST is currently working within the SGIP and the networking-related Priority Action Plans such as PAP1, PAP2, PAP15, and PAP18 on expediting the identification and development of network standards in support of reliable and robust Smart Grid communication infrastructures and developing end-to-end communication requirements for Smart Grid applications. Recently, PAP2 produced the NIST Interagency Report 7761, *Guidelines for Assessing Wireless Standards for Smart Grid Applications*, v. 1.0. For more information, including how to participate, please visit: <http://www.nist.gov/smartgrid/>.



Cybersecurity in the Smart Grid

Emerging cyber threats that target power systems have highlighted the need to integrate more advanced security to protect these critical assets. To address the cross-cutting issue of cybersecurity, NIST established the SGIP Cyber Security Working Group (CSWG). The CSWG now has more than 625 participants, and is composed of national and international members from the private sector (including utilities, vendors, and service providers), academia, regulatory organizations, state and local government, and federal agencies. In August 2010, the CSWG produced NIST Interagency Report 7628, *Guidelines for Smart Grid Cyber Security*. Since then, the group has moved on to focus on specific topics such as risk management processes, key management within the Smart Grid, developing a Smart Grid security architecture, testing and certification issues, Advanced Metering Infrastructure security, and privacy within the Smart Grid. One subgroup has also conducted reviews of several Smart Grid-related standards to see how these standards address cybersecurity.

A biweekly conference call is held by the CSWG chair to update the members on the subgroups, SGIP activities, and related information. Subgroups hold regular conference calls while actively working on a project. Information on the CSWG, subgroups, outreach, how to participate, and all associated documents may be found at: <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG>.