NIST finalizes initial set of smart grid cyber security guidelines

September 15 2010

The National Institute of Standards and Technology has issued its first Guidelines for Smart Grid Cyber Security, which includes high-level security requirements, a framework for assessing risks, an evaluation of privacy issues at personal residences, and additional information for businesses and organizations to use as they craft strategies to protect the modernizing power grid from attacks, malicious code, cascading errors and other threats.

The product of two formal public reviews and the focus of numerous workshops and teleconferences over the past 17 months, the three-volume set of guidelines is intended to facilitate organization-specific Smart Grid cyber security strategies focused on prevention, detection, response and recovery.

The new report was prepared by the Cyber Security Working Group (CSWG) of the Smart Grid Interoperability Panel, a public-private partnership launched by NIST with American Recovery and Reinvestment Act funding from the Department of Energy. The guidelines are the second major output of NIST-coordinated efforts to identify and develop standards needed to convert the nation's aging electric grid into an advanced, digital infrastructure with two-way capabilities for communicating information, controlling equipment and distributing energy.

"These advisory guidelines are a starting point for the sustained national effort that will be required to build a safe, secure and reliable Smart

Grid," said George Arnold, NIST's national coordinator for Smart Grid interoperability. "They provide a technical foundation for utilities, hardware and software manufacturers, energy management service providers, and others to build upon. Each organization's implementation of cyber security requirements should evolve as technology advances and new threats to grid security arise."

The report advocates a layered—or "defense in depth"—approach to security. Because cyber security threats are diverse and evolving, the report recommends implementing multiple levels of security.

The guidelines identify 137 interfaces—points of data exchange or other types of interactions within or between different Smart Grid systems and subsystems. These are assigned to one or more of 22 categories on the basis of shared or similar functional and security characteristics. In all, the report details 189 high-level security requirements applicable either to the entire Smart Grid or to particular parts of the grid and associated interface categories.

All three volumes of Guidelines for Smart Grid Cyber Security (NISTIR 7628) can be downloaded at: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

Under the Energy Independence and Security Act of 2007, Congress assigned NIST to coordinate development of a framework that would enable a Smart Grid that is safe, secure and interoperable from end to end. In its January 2010 report, NIST described a high-level conceptual reference model for the Smart Grid, identified existing or emerging standards relevant to the ongoing development of an interoperable Smart Grid, and spelled out several high-priority standards-related gaps and issues that NIST and its partners are now addressing.