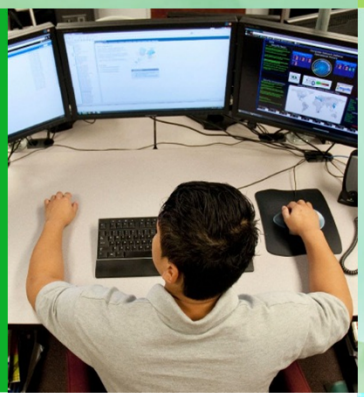
The primary goal of the CSWG is to develop a cybersecurity risk management strategy for the Smart Grid to enable secure interoperability of solutions across different domains/components.

Smart Grid Interoperability Panel (SGIP)

CyberSecurity Working Group (CSWG)



The major elements of the Smart Grid, in addition to the grid that carries the electricity, are the information technology, the industrial control systems, and the communications infrastructure used to send command information across the grid from generation to distribution systems. These elements are also used to exchange usage and billing information between utilities and their customers. Key to the successful deployment of the Smart Grid infrastructure is the development of the cybersecurity strategy for the Smart Grid. In fact, cybersecurity needs to be designed into the new systems that support the Smart Grid, and added into existing systems. The electric grid is critical to the economic and physical well being of the nation, and emerging cyber threats targeting power systems highlight the need to integrate advanced security to protect critical assets.

CYBERSECURITY IN THE SMART GRID

The National Institute of Standards and Technology (NIST) established the SGIP CyberSecurity Working Group (CSWG) in support of the Energy Independence and Security Act of 2007 to address the cross-cutting issue of cybersecurity. The CSWG has more than 650 participants worldwide from the private sector (including utilities, vendors, and service providers), academia, regulatory organizations, state and local government, and U.S. federal agencies.

The CSWG membership collaborated to deliver the NIST Interagency Report 7628, *Guidelines for Smart Grid Cyber Security,* in August 2010. Since then the group has focused on specific topics, such as risk management processes, key management in the Smart Grid, the Smart Grid security architecture, security testing and certification, Advanced Metering Infrastructure security, and privacy in the Smart Grid. In addition, the group is conducting security reviews of many Smart Grid-related standards.

An open conference call is hosted biweekly by the CSWG chair to update the members on subgroup status, SGIP activities, and other related information.

Membership in the CSWG is open to all. There are no dues, and there is no required time commitment. Many members participate from around the world by monitoring the minutes and email conversations of the subgroups.

MAKING THE CONNECTIONS

Because cybersecurity issues directly affect many areas in the Smart Grid, the CSWG designated liaisons to the Smart Grid Architecture Committee (SGAC), the Smart Grid Testing and Certification Committee (SGTCC), and the Priority Action Plans (PAPs). Many members actively participate in the above committees, the PAPs, and the Domain Expert Working Groups (DEWGs) in the Smart Grid Interoperability Panel (SGIP).

The CSWG also maintains connections with organizations such as the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG), the North American Electric Reliability Corporation (NERC), the Federal Energy Regulatory Commission (FERC), the National Electric Sector Cybersecurity Organization (NESCOR), the Department of Energy (DOE), and the National Association of Regulatory Utility Commissioners (NARUC).

SGiP SMART GRID INTEROPERABILITY PANEL

THE NISTIR 7628 V1.0

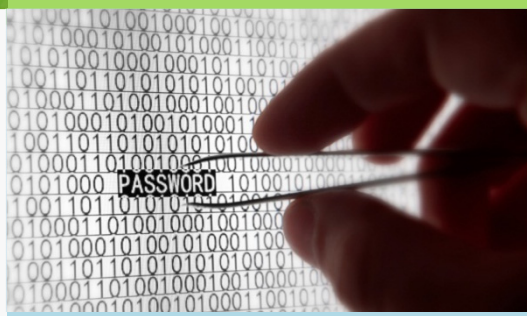
The CSWG's initial deliverable, the three-volume NIST Interagency Report 7628 (NISTIR 7628), presents an analytical framework that organizations can use to develop effective cybersecurity strategies tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities. Organizations in the diverse community of Smart Grid stakeholders—from utilities to providers of energy management services to manufacturers of electric vehicles and charging stations—can use the methods and supporting information presented in the report as guidance for assessing risk, and then identifying and applying appropriate security requirements to mitigate that risk.

THE CSWG SUBGROUPS

During the development of NISTIR 7628, the subgroups performed detailed technical analysis on an array of security-related topics, and then documented the research, issues, and guidance in specific sections. The approach taken by all subgroups is an open and collaborative process in which any CSWG member is welcome to participate and contribute.

The CSWG creates and disbands subgroups as needed to meet present needs. Since the NISTIR 7628 v1.0 publication, some of the CSWG subgroups were merged, while others are regrouping as they determine their next set of tasks. The CSWG currently consists of the following subgroups:

- The **Advanced Metering Infrastructure (AMI) Security subgroup** plans to create a set of AMI security requirements.
- The **Architecture subgroup** focuses on the enhancement of the logical security architecture for the Smart Grid. This group's work is used as input to the SGIP Architecture Committee.
- The **Design Principles subgroup** continues the work of identifying bottom-up problems and design considerations developed by the former Bottom-up, Vulnerability, and Cryptography and Key Management subgroups.
- The **High-Level Requirements subgroup** addresses the procedural and technical security requirements of the Smart Grid to be addressed by stakeholders in Smart Grid security. To create the initial set of security requirements in NISTIR 7628 v1.0, this subgroup adapted industry-accepted security source documents for the Smart Grid.
- The **Privacy subgroup** continues to investigate privacy concerns between utilities, consumers, and non-utility third-parties.
- The **Standards subgroup** assesses standards and other documents with respect to the cybersecurity and privacy requirements from NISTIR 7628. These assessments are performed on the standards contained in the NIST Special Publication 1108, *Framework and Roadmap for Smart Grid Interoperability Standards,* or in support of the PAPs.
- The **Testing and Certification subgroup** establishes guidance and methodologies for cybersecurity testing of Smart Grid systems, subsystems, and components.



LEARNING MORE AND GETTING INVOLVED

We welcome your participation in the CSWG. Below are resources to help you get involved:

Learn more about the CSWG: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG

Learn more about the subgroups, including meeting times: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WorkingGroupInfo

To join the CSWG and any of the subgroups, send your name, affiliation, and which lists you wish to join to: *tbrewer@nist.gov* and *marianne.swanson@nist.gov*

Download NISTIR 7628 at: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628

SGiP SMART GRID INTEROPERABILITY PANEL