

NIST Smart Grid Program

NIST and The Cybersecurity Working Group (CSWG)

**Jim St. Pierre, Deputy Director
Information Technology Laboratory**

May 16 – 17, 2012

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

1

Cyber Security Working Group (CSWG) Background

- To address the cross-cutting issue of cybersecurity, NIST established the Cyber Security Coordination Task Group (CSCTG) in March 2009.
- Moved under the NIST Smart Grid Interoperability Panel (SGIP) as a standing working group and was renamed the Cyber Security Working Group (SGIP–CSWG).
- The CSWG now has more than 700 participants from the private sector (including vendors and service providers), academia, regulatory organizations, national research laboratories, and federal agencies.

NIST smart grid program

2

The CSWG Management Team

- Marianne Swanson – NIST Chair
- Matthew Light – DOE, Vice Chair
- John Lim – New York Consolidated Edison, Vice Chair
- Dave Dalva – Vice Chair
- Mark Enstrom – NeuStar, Secretary
- Tanya Brewer – NIST
- Victoria Pillitteri – Booz Allen Hamilton

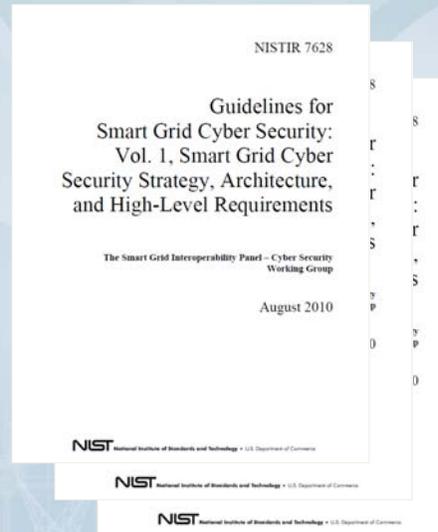
CSWG Active Sub-groups and Leads

- **AMI Security Group**
 - Doug McGinnis
- **Architecture Group**
 - Elizabeth Sisley
- **Design Principles Group**
 - Daniel Thanos & Annabelle Lee
- **High-Level Requirements Group**
 - Dave Dalva & Victoria Pillitteri
- **Privacy Group**
 - Rebecca Herold
- **Security Testing and Certification Group**
 - Nelson Hastings
- **Standards Group**
 - Frances Cleveland

Guidelines for Smart Grid Cyber Security

NIST Interagency Report
7628 - August 2010

- Development of the document lead by NIST
- Represents significant coordination among
 - Federal agencies
 - Private sector
 - Regulators
 - Academics



Recent Accomplishments - 1

- SGIP Priority Action Plan (PAP) collaboration
- Ongoing outreach and education efforts
 - 8 States (4 PUCs)
 - Over 1,000 participants
 - One page brochure
 - Privacy briefing for utilities and public utility commissions
- Collaborated with DOE and NERC to develop a harmonized electricity sector enterprise-wide risk management process

Recent Accomplishments - 2

- CSWG/DOE's NESCOR collaboration on SEP 1.0 and 1.1 technical white paper
- Cybersecurity Review of Standards
 - Over 60 reviews of standards or PAP deliverable requirements, for example:
 - 5 IEC Common Information Model Standards
 - ZigBee SEP 1.0, 1.1, and Draft SEP 2.0
 - ANSI C12 Suite
 - IEC 1815 (DNP3) and IEC 1815.1 (Mapping between DNP3 and IEC 61850)
- White Paper on Automating Smart Grid Security
- Draft NERC CIP v5 mapping to NISTIR 7628
- Mapping and analysis between NISTIR 7628 and the Smart Meter Gateway Protection Profile

NIST smart grid program

Continuing Work

- Analyzing AMI use cases to determine detailed AMI security requirements.
- Developing a “Recommended Practices” chapter on best ways to protect privacy when sharing data with third parties.
- Drafting a NISTIR on testing criteria for the NEMA Upgradeability Standard.

8

NIST smart grid program

Cyber-Physical Attacks - Collaboration

- The CSWG will provide cybersecurity expertise to help address cyber-physical threats in coordination with other federal agencies and industry groups.
 - Workshop April 23 – 24, 2012 in Gaithersburg, MD
- The collaborative effort will result in:
 - NISTIR 7628 high-level security requirements being augmented to address cyber-physical security threats.
 - NISTIR on workshop proceedings.
 - Suggested future work/collaboration in this area.

Potential Future Work - 1

- Security Content Automation Protocol (SCAP) extension to cover cyber-physical systems
 - Provide a standardized, measureable, automated method of continuous monitoring for Smart Grid components, increasing efficiency and accuracy, reducing costs of secure implementations, and improving capability and interoperability of implementations
- Research in lightweight, low-power cryptography
 - Enabling encryption for millions of smart meters and other devices for the Smart Grid with limited computational power

Potential Future Work - 2

- Identity management
 - Helping to ensure the security of customer information when dealing with utilities and third parties; enabling remote authentication on anonymous devices

NIST smart grid program

Learning More and Getting Involved

- Learn more about the CSWG at: <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: tanya.brewer@nist.gov and marianne.swanson@nist.gov
- Download NISTIR 7628 at: <http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628>

NIST smart grid program

12

Additional Links to Documents

- SCAP White Paper: http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CyberSecurityCTG/Automating_Smart_Grid_Security_v1_4.pdf
- Privacy PUC Training Slides: [CSWG Smart Grid Privacy Training for PUCs December 14 2011 FINAL.pptx](#):
- DOE Risk Management Process Guideline: <http://energy.gov/sites/prod/files/RMP%20Guideline%20Second%20Draft%20for%20Public%20Comment%20-%20March%202012.pdf>

NIST smart grid program

Questions?

NIST smart grid program

14