

Cyber Security Working Group

Smart Grid Interoperability Panel - Cyber Security Working Group

Brian Lenane

Information Technology Laboratory

National Institute of Standards and Technology (NIST)



Energy Independence and Security Act

- In the Energy Independence and Security Act (EISA) of 2007, Congress established the development of a Smart Grid as a national policy goal.
- Under EISA, NIST is directed to “*coordinate the development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems*” as well as maintain the reliability and security of the electricity infrastructure.

Cyber Security Working Group (CSWG)

- To address the cross-cutting issue of cyber security, 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 650 participants from the private sector (including vendors and service providers), academia, regulatory organizations, national research laboratories, and federal agencies.

The CSWG Management Team

- Marianne Swanson – NIST Chair
- Matthew Light – DOE, Vice Chair
- John Lim – Consolidated Edison of NY, Vice Chair
- Dave Dalva – Booz Allen Hamilton, Vice Chair
- Mark Enstrom – NeuStar, Secretary
- Tanya Brewer – NIST
- Victoria Yan – Booz Allen Hamilton
- Sandy Bacik – EnerNex

CWSG Active Sub-groups and Leads

- **AMI Security Group**
 - Doug McGinnis & Sandy Bacik
- **Architecture Group**
 - Sandy Bacik
- **Design Principles Group**
 - Daniel Thanos & Annabelle Lee
- **High-Level Requirements Group**
 - Dave Dalva & Victoria Yan
- **Privacy Group**
 - Rebecca Herold
- **Security Testing and Certification Group**
 - Nelson Hastings & Sandy Bacik
- **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

NISTIR 7628 – What it IS and IS NOT

What it IS

- A tool for organizations that are researching, designing, developing, and implementing Smart Grid technologies
- May be used as a guideline to evaluate the overall cyber risks to a Smart Grid system during the design phase and during system implementation and maintenance
- Guidance for organizations
 - Each organization must develop its own cyber security strategy (including a risk assessment methodology) for the Smart Grid.

What it IS NOT

- It does not prescribe particular solutions
- It is not mandatory

Recent Accomplishments

➤ Recent Activities

- SGIP Priority Action Plan (PAP) collaboration
- Ongoing outreach and education efforts
 - 8 States (4 PUCs)
 - Over 1000 participants
- CSWG Three Year Plan updated
- Developing a NISTIR 7628 High Level Requirements Assessment Guide
- Collaborated with DOE and NERC to develop a harmonized energy sector enterprise-wide risk management process
- Participating in the IEC62443 2-4

➤ Cyber Security Review of Standards

- Completed:
 - Over 25 reviews of standards or PAP deliverable requirements
 - 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)
- Future:
 - NAESB REQ 21
 - MultiSpeak

Continuing Work

- Analyzing AMI use cases to determine detailed AMI security requirements.
- Coordinating with the SGIP Smart Grid Test and Certification Committee (SGTCC) to develop guidance and recommendations on Smart Grid conformance, interoperability, and cybersecurity testing.
- CSWG/DOE's NESCOR collaboration on SEP 1.0 and 1.1 technical white paper.
- Privacy subgroup developing a "Best Practices" document on best ways to protect privacy when sharing data with third parties

Cyber-Physical Attacks – Collaboration

- Assessing the impact of cyber-physical attacks will require expertise in:
 - Cybersecurity
 - Physical security
 - The electric infrastructure
- The CSWG will provide cybersecurity expertise to help address cyber-physical threats in coordination with other federal agencies and industry groups.
 - Draft white paper on research and path forward
 - Workshop planned for April 23 - 24 2012
- It is anticipated that this collaborative effort may result in the NISTIR 7628 high-level security requirements being augmented to address cyber-physical security threats.

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:
tbrewer@nist.gov and marianne.swanson@nist.gov
- Download NISTIR 7628 at:
<http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628>



Questions?