NIST and the Cyber Security Working Group

Marianne Swanson, Chair
Smart Grid Interoperability Panel - Cyber Security Working Group
Computer Security Division
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 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 650 participants from the private sector (including vendors and service providers), academia, regulatory organizations, national research laboratories, and federal agencies.

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

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
  - Privacy subgroup developing a "Best Practices" document on best ways to protect privacy when sharing data with third parties
  - Coordination with DOE's NESCO and NESCOR groups
  - Coordination with the ASAP-SG
  - Task force developed to harmonize proposed work item IEC 62443-2-4 with NISTIR 7628

- Cybersecurity Review of Standards
  - Completed:
    - Over 20 reviews of standards and PAP deliverable requirements
      - 5 IEC Common Information Model Standards
      - SEP 1.0, 1.1 and Draft 2.0
  - Future:
    - Renewable Standards
    - IEC 1815 (DNP3) and IEC 1815.1 (Mapping between DNP3 and IEC 61850)

Continuing Work

- Collaborating with DOE and NERC to develop a harmonized energy sector enterprise-wide risk management process.
- 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.
- Developing a virtual test environment for the NEMA upgradeability standard.
- Developing a NISTIR 7628 High Level Requirements Assessment Guide.

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
- 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.

How to get involved

- To join the CSWG mailing list, contact:
  - Marianne Swanson (marianne.swanson@nist.gov)
  - Tanya Brewer (tanya.brewer@nist.gov)

- All are welcome to dial into the CSWG conference calls
  - Teleconference Day & Time: Biweekly on Mondays, 11am Eastern Time
  - Call-in number: 866-793-6322
  - Participant passcode: 3836162

- CSWG TWiki: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG

Questions?