Smart Grid Interoperability Panel – Cyber Security Working Group
Meeting Minutes (May 16, 2011)

NIST LEAD: Marianne Swanson
If you want to be on an email list, contact Marianne and Tanya.

NIST Contacts:
Marianne Swanson, marianne.swanson@nist.gov
Tanya Brewer, tbrewer@nist.gov
Victoria Yan, yan_victoria@bah.com

SGIP-CSWG Administration
Vice Chairs:
- Dave Dalva, didalva@gmail.com
- Alan Greenberg, Alan.M.Greenberg@boeing.com
- Matt Light, Matthew.Light@hq.doe.gov
Secretary: Mark Enstrom, mark.enstrom@neustar.biz

SGIP-CSWG SubGroups Information:
Listed below are the SGIP-CSWG leads for each group. More detailed information about each group is available at http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WorkingGroupInfo. If you would like to join any of these subgroups, please let Marianne and Tanya know and you will be added to the group(s).

Current Standing Subgroups

Architecture Group
CSWG Leads: Sandy Bacik

Design Principles Group
CSWG Lead: Daniel Thanos and Annabelle Lee

High Level Requirements Group
CSWG Leads: Dave Dalva and Victoria Yan

Privacy Group
CSWG Leads: Rebecca Herold

R & D Group
CSWG Leads: Isaac Ghansah and Daniel Thanos

Standards Group
CSWG Leads: Frances Cleveland

Testing and Certification Group
CSWG Leads: Nelson Hastings and Sandy Bacik

CSWG/SGSEC AMI Security Group
CSWG Leads: Sandy Bacik and Ed Beroset
Remember:
Please mute your phone when not speaking, and please do not put the call on hold as we will hear the hold music. Thank you.

Standards subgroup
The group has been very busy with standards reviews, and has just finished the review of ANSI C12.22 and Zigbee SEP 2.0, draft version 0.7. They are currently working on Zigbee SEP 1.0 and 1.1, with a number of experts, many from the new PAP 18. These reviews will hopefully be done within 2 weeks. Marianne sent an email to Tobin to get a copy of the Carnegie Mellon security review of Zigbee SEP 1.0 to aid our work.

The group is starting the review of PAP 12-related standards: IEEE 1815 (DNP3) and IEEE 1815.1 (mapping between DNP3 and IEC 61850).

The group still needs some missing pieces of PAP 15 documents – IEEE 1901. The ITU document is available on the ANSI portal.

The group will soon start working on the PAP 11 standards from SAE. We need to have a few voting members of SAE in order to review the documents. If you’re interested, please contact Frances Cleveland.

Finally, the new Twiki page is up; it should now be clearer as it has gone through a cleanup.

Testing and Certification subgroup
The group is writing assessment guidance regarding conformance to NISTIR 7628. The group will use NIST SP 800-53A as a guideline.

Marianne would like to see the CSWG use the SGIP document structure for the deliverable, which is currently in the developmental process within the SGIP; an overview slide showing current status is provided below. Please note that this has not yet been voted on by the SGIP Governing Board, and is provided for information only. When it is approved, the CSWG will use this structure for externally released documents.
SGIP DOCUMENT BRANDING

- Plenary Secretary Function
  - Tracking and logging of SGIP work products
  - Control over the mark
- Sources
  - SGIP Leadership, including
    - Deliverables from SGIP Officers
    - SGIP Standing Committees
    - SGIP Working Groups
      - Domain Expert Working Groups
      - Priority Action Plan Working Groups
  - SGIP Governing Board, including
    - Deliverables from GB Officers
    - GB sub-committees
- Essential Elements
  - Formatting & Style
  - Disclaimers
    - “THIS IS NOT A NIST DOCUMENT”
  - Maintenance Instructions
  - Revision History
  - Citation Instructions

AMI subgroup

The group reviewed the first use case, which dealt with operational commands to the meter. The group reviewed the use case and verbiage, and sent that on. The group will now start the review of the non-operational commands use case, and will be addressing failure analysis on the operational commands to the meter.

IEC 62443-2-4 Proposed New Work Item

Mike Ahmadi proposed a new work item for the group. IEC 62443 2-4 is a new effort in TC65. This looks like a new set of high-level requirements that a vendor could use to confirm if a product meets requirements.

Southern Company has asked that vendors certify to this standard; other utilities are also interested. This was submitted as a work product to IEC, and therefore should be reviewed by CSWG to ensure that the requirements in this document align with the high-level security requirements of the NISTIR. With regards to timing, this will be in the IEC comment period until September, and will then go through the comment resolution period.
Questions that need to be asked include:
- Are there any conflicts?
- Are there items in the WIB or IEC standard that are missing in the NISTIR? Those should be flagged.
- Are there things in the NISTIR missing from the IEC standard?
- Is anything missing from both?

Mike has many people interested in this work and is in the process of gathering comments. He would like to align this with the work going on in the Testing and Certification group.

Marianne commented that we want to be aligned with the IEC, as we need to make sure this is addressed in the right place. They are presenting this as a certification for testing and are including high-level requirements. That implies that this should be coordinated with the Testing and Certification group and the High-level Requirements group.

The CSWG may form a joint group on a temporary basis; this group may submit comments for the CSWG as a collective whole. The group will have a linkage to high-level requirements; once tweaked the testing and certification group could make adjustments.

Mike Ahmadi is willing to take the leadership role for this group, as he is officially on the TAG, and will be working on comments. Mike emphasized that June 17 is the deadline for comments and our time is rather short. The group will need to come up with a cross walk or a one-to-one mapping to determine what’s missing and what needs to be added. Mike wants some help doing this review, etc.

Please note that if you’re working on this, do not post IEC information on the Twiki. The temporary working group will discuss ways to share it. If you want to participate, let Tanya know and she will add you to the HLR working group. Tanya, Vicky, and Mike will work off line to set up the right time.

**White House Cyber Security Legislation**

Marianne wanted everyone to be aware that the White House released a proposed cyber security legislation document which addresses many items including CIP and voluntary regulations.

**ASAP SG**

Darren Highfill wanted to mention that he is putting the last touches on the wide area monitoring and control security profile from ASAP SG. This is unique because they have requirements that build on the NISTIR 7628. He will send to Marianne, and she will distribute it to the CSWG for comments.
Outreach

The next outreach session is this week on the 18th and 19th at the University of Minnesota. The CSWG will present on the 18th.

Next Call

The next call will be on 6 June.

Thank you!

Next call for the SGIP-CSWG: Monday, June 6, 2011 at 11:00 EST
Call-in number: 866-793-6322    Participant passcode is: 3836162
Please remember to mute your phones when not speaking.