Smart Grid Interoperability Panel – Cyber Security Working Group  
Meeting Minutes (February 7, 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, ddalva@cisco.com  
- Alan Greenberg, Alan.M.Greenberg@boeing.com  
- William Hunteman, William.Hunteman@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](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).

### Standing Subgroups

<table>
<thead>
<tr>
<th>Group</th>
<th>CSWG Lead(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architecture Group</td>
<td>Sandy Bacik</td>
</tr>
<tr>
<td>Bottom Up Group</td>
<td>Andrew Wright and Daniel Thanos</td>
</tr>
<tr>
<td>Crypto and Key Management Group</td>
<td>Daniel Thanos, Doug Biggs, and Tony Metke</td>
</tr>
<tr>
<td>Design Principles Group</td>
<td>Daniel Thanos and Annabelle Lee</td>
</tr>
<tr>
<td>High Level Requirements Group</td>
<td>Dave Dalva and Victoria Yan</td>
</tr>
<tr>
<td>Privacy Group</td>
<td>Rebecca Herold</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group</th>
<th>CSWG Lead(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>R &amp; D Group</td>
<td>Isaac Ghansah and Daniel Thanos</td>
</tr>
<tr>
<td>Standards Group</td>
<td>Frances Cleveland</td>
</tr>
<tr>
<td>Vulnerabilities Group</td>
<td>Matt Carpenter and Matt Thomson</td>
</tr>
<tr>
<td>Testing and Certification Group</td>
<td>Nelson Hastings, Sandy Bacik</td>
</tr>
<tr>
<td>CSWG/SGSEC AMI Security Group</td>
<td>Darren Highfill and Ed Beroset</td>
</tr>
</tbody>
</table>
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.

FERC Technical Conference
The FERC Technical Conference took place on Monday, January 31. The meeting was webcast live; the audio archive of the meeting can be found here: http://www.capitolconnection.net/capcon/ferc/ferc.htm

The general take away from the meeting is that there is no current consensus on the standards, or on the meaning of FERC standards adoption. NIST, the SGIP, and FERC will need to get that answered before we can articulate the next steps.

The general themes from the meeting were as follows:
- We (the many stakeholders) have done a lot of good work, but we need to drive for further consensus.
- Some stakeholders believe that their input should have a higher weighting as they have been in the industry longer and have a bigger stake in the outcome.
- There is a lot more work to be done on standards: there are 25 additional standards in the framework document and 75 additional standards beyond that.
- There is a need for more marketing and education. Many people do not know about the SGIP and/or its tools and processes.
- Utilities are asking for rate support from the commissions to allow them to get more involved in the standards processes.
- Utilities would like to add an additional check off layer to the process to give them more of a chance to review.

FERC has a 3 month comment period open. Please refer to Marianne’s email for clarification. People are highly encouraged to submit comments to FERC.

ENERNEX and the NIST team will be meeting in Knoxville this week to discuss ways to enhance the process.

Risk Management Initiative
Members of the CSWG will be working in the Risk Management Framework initiative with representatives from NIST, DOE, NERC, DHS, and the utility industry (EEI, APPA, IOUs, etc). The goal of the initiative is to tailor the NIST SP 800-39 to the utility sector, and provide a common language for the smart grid stakeholders. The group will look at enterprise-wide risk and will take a 3 tiered approach along the lines of 800-39.

The group will start off with a core team that will develop a straw man framework. This will then be sent to a larger review team for a sanity check. The draft should be complete by the end of the summer.
Three Year Plan

Marianne and the management team are currently working on the three year plan. The goal is to get the draft out by the end of this week; comments are due back in time for the response to the GAO by the 25th of February.

Marianne does need input from the various sub groups regarding their plans. Specifically, we need input from the R&D and Vulnerability subgroups.

Outreach

The Outreach team will be in Baltimore at UMBC on the 15th February. All are welcome. For information on the event, please see the agenda on the Twiki.

http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/UMBCAgendaAndLogistics

The outreach session at the Texas PUC will be coming up on the 23rd of February. Please see that and other upcoming events at the following link.

http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSWGOutreach

SAE J 2931 PEV Standard: Inband Signaling Communication for Plug-in Electric Vehicles

The group is looking for more involvement from people who have cyber security knowledge. If you are interested, please let Mike Coop know.

Privacy subgroup

The multiple sub teams continue their work.

- The NSTIC team is on hold until the framework is updated.
- The use case team continues to work and make good progress.
- The PEV team is getting involved with other group outside the CSWG to provide more perspective.
- The 3rd party data team is close to completing their work.
- A new group is forming to work on training and awareness within the smart grid.

The full group will now meet on the 1st and 3rd Thursdays of each month.

Congratulations to Rebecca for being named one of the best privacy advisors for 2010 by Computerworld.

**Design Principles subgroup**

Update given by Mike Ahmadi. The majority of the last discussion was regarding the FERC webcast and a discussion of the cost to get copies of the standards. Not many in the group have had the opportunity to review standards.

For the DPG document, the group categorized the topics into 5 major categories. Group members are asked to choose the topics they want to work with. The topics are:

- Crypto and key management
- Security detection and response
- Vulnerability
- Trusted HW and SW
- Design process.

Annabelle wanted to mention federal legislation, HR-174, which may give DHS a new office looking at cyber security infrastructure.

**Testing and Certification subgroup**

The group is completing the documents to give to the SGTCC, as well as finishing up the RFC questionnaire for use by the utilities. This will be posted on the Twiki.

The group has listed the test case topics, and is reviewing requirements to make sure they are testable and actionable.

**AMI Security subgroup**

The group is establishing a format to review testing level criteria for the requirements in the AMI security profile. They are close to completing the format and template for the security requirements. Once that is completed they will put together a plan for AMI. This will be shared with the Testing and Certification sub group and will be posted to the Twiki.

**Standards subgroup**

The group is getting ready to release ANSI 12.1 and 12.19 to the SGTCC. The C12.22 review should be complete by the end of next week.

Once all reviews are completed, they will be posted on the Twiki. The target is to do this by the 14th. When done they will put out a note to the CSWG and to the SGIP to ask members to review. Note that if people need access to the standards, they will have to ask, as there are a limited number of slots. Once people are done reviewing a standard, they will need to give up the slot so someone else can access the standards. Reviewers will have to agree to ANSI access requirements.
There will be a comment form available. Please note that this is only a cyber security review against criteria in the NISTIR, and not a physical-cyber review.

For more information, please contact Sandy Bacik and/or reference the following page:
http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPMemberAccessToANSIPortal

Next Call
The government will be closed on 21st February for the President’s Day holiday. The next CSWG call will be on 28 February 2011.

Thank you!

Next call for the SGIP-CSWG: Monday, February 28, 2011 at 11:00 EST
Call-in number: 866-793-6322  Participant passcode is: 3836162
Please remember to mute your phones when not speaking.