Smart Grid Interoperability Panel – Cyber Security Working Group
Meeting Minutes (08 March 2010)

NIST LEAD: Annabelle Lee
If you want to be on an email list, contact Annabelle and Tanya

NIST Contacts:
Annabelle Lee, annabelle.lee@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
Secretary: Mark Enstrom, mark.enstrom@neustar.biz

SGIP-CSWG Sub-Groups 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 sub-groups, please let Annabelle and Tanya know and you will be added to the group(s).

Standing Sub-groups
Architecture Group
CSWG Leads: Justin Searle and Sandy Bacik

Bottom Up Group
CSWG Leads: Andrew Wright and Daniel Thanos

High Level Requirements Group
CSWG Leads: Tom Overman and Dave Dalva

Privacy Group
CSWG Leads: Gal Schpantzer and Rebecca Herold

R & D Group
CSWG Leads: Jessica Ascough and Isaac Ghansah

Standards Group
CSWG Leads: Ramesh Reddi and Virginia Lee

Vulnerabilities Group
CSWG Leads: Matt Carpenter and Matt Thomson

Crypto and Key Management Group
CSWG Lead: Daniel Thanos and Doug Biggs
SGIP-CSWG Made a Good Showing at RSA

Annabelle and a few other CSWG participants were on panels and in attendance at the RSA Conference in San Francisco the week of 1 March 2010. As expected given the current focus on security, the conference itself was very well attended. While there, NIST management and Annabelle received many good comments on the NISTIR, including good comments from Intel.

Congratulations to the team!

NISTIR 7628 v1.0 Release Delayed

The Federal Register Notice, a requirement to open up the comment period, is likely delayed until the week of 15 March 2010. Given the 60 day comment period following the release of the FRN, the version 1.0 draft is now targeted for the 3rd or 4th week of May. The release will then have to go through an internal NIST review; therefore the final document release is likely to be in the middle of June 2010.

Boeing has offered the time and efforts of a technical editor to help the NISTIR conform to a single style sheet. The person is working through the document right now.

Thank you Boeing!

SGIP-CSWG Face to Face Scheduling

The face to face was originally targeted for 12 – 13 April. With the delay noted above, the F2F is now tentatively targeted for the week of 17 May 2010. The final date and location are being determined, and will be scheduled to not conflict with Connectivity Week (24 May).

Please let Annabelle know of any other conferences or meetings that may conflict in May. Given the plethora of meetings, not all conflicts will be resolved.

Also please let Annabelle know if your company or organization would be interested in hosting the meeting. We will need 1 big meeting room, 6 – 8 breakout rooms, and conference bridge/telecom capabilities for each room. Expected attendance will be between 60 and 80 people; 100 people is the maximum.

SGIP Meeting in Chantilly, VA

The meeting will be taking place next week on 16 – 17 March 2010, in Chantilly, VA. The SGIP, the priority action plans, the standing committees, and the CSWG will all be meeting there. Since there is a need for information sharing across many groups, Annabelle will be sending people to sit in on various meetings of other groups. There will be telecom and webinar capabilities – so all can participate.
Call for Participation

Annabelle is putting out the call for more people to get involved in the working groups. The current crew has put in a lot of time and great effort, but they need a break. Also, the document would benefit greatly from fresh energy and a fresh perspective.

Please get involved! If you are interested – send Annabelle and Tanya an email – and let them know the specific groups you are joining.

Comprehensive National Cybersecurity Initiative Summary

As announced at the RSA Conference, the Comprehensive National Cybersecurity Initiative Summary was posted on the White House web site. (http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative)

The document is about 5 pages long, and is a good high level read of the programs that were established in the previous administration and are still of high priority to the federal government.

GRC Documents

The Federal Information Security Management Act (FISMA) is being updated. This will require the Governance, Risk, and Compliance (GRC) requirements to be updated and tailored to the new FISMA. Annabelle is looking for volunteers to help with that.

(Update: Annabelle found out that the approach may be different – and may not involve revising FISMA.) Regardless – the GRC requirements in our NISTIR need a good scrub. All volunteers please contact Annabelle and Tanya.

Be Careful What’s Included in the NISTIR

From the FBI talk at the RSA Conference, Cyber terrorism and Cybercrime are both on the rise. While this is not a surprise, it does remind us that there is an increased chance of a combined cyber security and physical attack. We need to be careful what we include in the NISTIR, including the threat models, as we do not want to give the “bad guys” a road map.

The thing to remember is that there is a difference between an individual and a well-funded nation-state. The nation-state is more organized, well funded, widespread, and is better able to attack the critical infrastructure. Also, the nation-state is more motivated to attack on a larger scale.

Therefore, we do not want to include information that can help the nation-state, or other well funded large organizations, to plan their attack.
AMI Security Profile and Third Party Access Draft

The group, led by Darren Highfill, finished the AMI Security Profile and Third Party Access draft document in December, and is looking for feedback.

The AMI Security profile documents can be found here

And here
http://www.smartgridipedia.org/images/d/d6/AMI_Security_Profile_-_v1_0.pdf

The Third Party Data Access Draft can be found here.

http://www.smartgridipedia.org/images/0/0d/3PDA_Security_Profile_-_v0_20_-_20100129.pdf

OSTP Blog

The White House Office of Science and Technology Policy (OSTP) blog now includes the OSTP Consumer Interface to the Smart Grid blog, located here http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/OSTPConsumerInterfaceSmartGrid#Ensuring_a_Positive_Customer_Con. This blog has seen a lot of traffic, much of which would be of interest to this group. Specifically, there is a lot of discussion of data ownership and control that can help inform the discussions in the Privacy Group.

There has also been some discussion of regulations and policies. Note that NIST can identify existing standards, policies, and regulations, but does not develop or mandate them.

DOE Funding

The Department of Energy has set up a website for organizations that were awarded SGIG and SGDP funding. The website is https://www.arrasmartgridcyber.net/index.php.

This site has a lot of information centered around Smart Grid Cyber Security and Interoperability, although the primary focus is on Cyber Security. It may be worth your while to view the website even if you were not awarded DOE funding.

Other RSA Conference Topics
There was a lot of buzz around cloud computing. The discussions covered transmission security versus storage security, public and private clouds, and security issues related to shared infrastructure.

Cryptography was another topic with some buzz, including a potential theoretical breaking of the advanced encryption standard. This will be covered in the Vulnerability group.

**Crypto and Key Management Working Group**

The Crypto Group had its initial call, with a lot of strong interest. The initial brainstorming call discussed the charter of the group, the content to be developed, and the content from the Bottom-Up group that can be reused. Notes from the call and Twiki content will be coming shortly.

The group is also looking for a co-lead – and Doug Biggs has volunteered. Welcome Doug and thanks.

**Bottom Up Group**

Two high level issues were addressed this week. First, the group is mapping the bottom up issues from the top level requirements; Stan and Vicky are doing a trial run. The second issue, software agent updates, may introduce significant issues as there is no control over them.

**Vulnerability Group**

Currently the group is mapping vulnerability classes to the DHS Catalog control classes.

**R&D Group**

The group has finished looking at the covert channels, and is now looking at steganographic tools and their applicability to cyber security (ex. Watermarks). Other research areas being addressed are DOS and DDOS, authentication and mitigation techniques, virtualization, and the cloud computing models.

**Standards Group**

Annabelle is working on getting access to standards. This is an issue and NIST management is aware of this.

The meeting itself has not had good attendance, and Virginia is looking for a new time for the meeting.

**Privacy Group**
The Privacy Group is dividing into teams to address the many issues that have come up in the group. Two topics with a lot of interest are data ownership and use case definition.

**Architecture Group**

Two main efforts are underway. First, the group is performing a check of the logical diagram. Second, the group is putting together the security architecture.

In addition, Justin and Sandy are participating in the SGIP – Architecture Committee. Annabelle will clarify with Fred Baker if the SGIP-AC will be focused on protocols.

**High Level Requirements Group**

This group will be a focus of Dave and Annabelle as the team starts to look specifically at refining the interface categories. FERC requested that the team identify critical and priority requirements. The group will work through a decision tree with one item to help clarify how to categorize items.

**Next call for the SGIP-CSWG:** Monday, March 15th, 11am EST.

**Call-in number:** 866-745-6097  **Participant passcode is:** 7413006

Please remember to mute your phones when not speaking.