CYBER SECURITY COORDINATION TASK GROUP
Meeting Minutes (14 December 2009)

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

CSCTG Sub-Groups Information:
Listed below are the CSCTG 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
CSCTG Leads: Justin Searle & Sandy Bacik

Bottom Up Group
CSCTG Leads: Andrew Wright & Daniel Thanos

High Level Requirements Group
CSCTG Lead: Annabelle Lee & Tom Overman

Privacy Group
CSCTG Lead: Gal Schpantzer & Rebecca Herold

R & D Group
CSCTG Leads: Jessica Ascough & Carl Gunter

Standards Group
CSCTG Lead: Ramesh Reddi & Virginia Lee

Vulnerabilities Group
CSCTG Leads: Matt Carpenter & Matt Thomson

FERC4+2 Sub-groups (on hold)

AMI Group
CSCTG Lead: Darren Highfill

DGM Group
CSCTG Lead: Jesus Molina

DR Group
CSCTG Lead: Ramesh Reddi

ES Group
CSCTG Lead: Andrew West

ET Group
CSCTG Lead: Stanley Klein

WASA Group
CSCTG Lead: Joe Bucciero

December 7th - 8th Working Meeting

Thank you to everyone who participated last week, both in person and by phone. It is always good to meet people face-to-face. We had over 60 individuals attend. Everyone was very productive, and there was a lot accomplished! Thank you again to Brent and the NeuStar folks, too! They did a fabulous job in hosting the meeting.

Comments on NISTIR 7628 Draft 1

Comments on the first draft of the NISTIR are being posted on the twiki as we get them. Topics covered in that comment should be evident from the file names used. Also, there is a summary sheet that lists the submitter and the commented sections of the NISTIR.
Please check the list to make certain you have seen all comments regarding the areas you are working on/interested in.

Draft NIST Framework Document

The NIST Framework Document is to be finished this week. We have two sections in this document—Cyber Security and Privacy. Annabelle has reviewed the privacy section, and this group has done a very nice job revising the section for the document. There was one comment on the risk management framework regarding the definition of cyber security that still needs addressing. The current one listed is IT heavy and does not include enough to cover the Smart Grid.

Suggestion per Daniel Thanos: List that “typically cyber security is defined as …”, but then go on to say “While it is true modern IT systems will have an important basis in the Smart Grid and their cyber security definition is preserved within their scope, once both the power and IT domain come together into the Smart Grid there is a new definition that is needed. Thus Cyber Security in the Smart Grid is further defined as an evolving framework of technologies (both power and cyber systems) and processes (in IT and power system operations and governance) that have at their foundation the preservation (at minimum) and enhancement of power system reliability through cyber means that exist in IT, communication, and power systems.”

Coordination with NERC

Annabelle has spoken with Keith Stouffer regarding the NERC CIP standards revisions. NERC CIP-002 is being revised this week by the NERC Standard Development Team (SDT) for the cyber security reliability standards. It will go out for public comment by the end of December 2009 for a 30 day informal comment period. NERC is expecting to receive industry feedback and revise the CIP-002 Standard before actually issuing the CIP-002 standard for formal industry comment, response, and balloting in the April 2010 timeframe. In parallel, the NERC SDT will be working on revisions to the remaining cyber security reliability standards (CIP-003 through 009).

In CIP-002, NERC is moving to use Low/Medium/High categorizations instead of Critical/Not Critical. They believe they may be able to use some of the work the CSCTG is putting out in the NISTIR document. In particular, they liked the “common controls” list of roughly 170 requirements that are applicable at an organizational level.

The goal is to have the initial draft of the replacement for the CIP-003 through CIP-009 (the catalogue of controls requirements) standards ready for industry feedback and comment by late-spring. The SDT is targeting to have all of the standards ready for approved by the end of 2010.

Glossary

The need for a comprehensive, cross-domain glossary was discussed. It was recommended to use the NERC glossary as a starting point. Annabelle will explore potential copyright issues with the IEC 62351 glossary.
Architecture Group
There are links on the twiki to each of the documents they are working on. They have reviewed and finished several diagrams, including the unified diagram showing all of the interfaces and the AMI diagram. (The chart is an eye test.)

Bottom Up Group
This group has been further refining their section of the NISTIR document. The ECC section has been fully revised. The roles and authentication sections need to be revised to make them more applicable to the SG. They are also going to include discussion about the need for a unified glossary.

High Level Requirements Group
This group has put out tentative impact levels for everyone to look at. Please give feedback on these if you have any.

Privacy Group
This group addressed all but two sets of comments during the face-to-face meeting. The other two sets, from EPIC and CDT, were lengthy. They are being addressed now. The material for the NIST Framework Document has also been revised.

R & D Group
There is now a list of 6 topics agreed upon by the group and a list of 6 possible topics to be discussed.

Standards Group
This group finished a disposition of the comments on their section of the NISTIR during the face-to-face meeting. They then began addressing comments on section 1 of the NISTIR document, which is also section 6 of the Framework Document.

Vulnerabilities Group
This group has made several updates to their section of the NISTIR document. One of the activities they have done is to make a list of potential types of readers of the NISTIR document.

Next call: Monday, December 21st, 11am EST.
Call-in number: 866-745-6097  Participant passcode is: 7413006
Please remember to mute your phones when not speaking.

No Call on December 28th (everyone enjoy the holidays).