CSWG/NIST Smart Grid Privacy Subgroup
June 8, 2012

Attendance:

- Rebecca Herold – Lead – The Privacy Professor
- Tanya Brewer – NIST
- Amanda Stallings – PUCO
- Paul Zumo – APPA
- Bruce McMillan – Missouri Univer. Science & Technology
- Marianne Rawls – NRECA
- Tony Munoz – Colorado PUC
- Ward Piles – Southern Co.
- Irene Gassko – FPL
- Brandon Robinson – on behalf of Southern Co.
- Dan Friedman – Amdocs
- Christine Hertzog – SmartGrid Library
- Ruth Yodaiken – FTC
- Ken Wacks – GWAC
- Anan Sokker – FPL

- SG UK Consultation Review – Amanda Stallings
- Determined that we would provide some feedback on that. Amanda and Chris are going to be looking at the document. The team has not had a chance to review the document to date. Please consider helping them review the document; it would be nice to have a different perspective other than from a regulatory stand-point. Trying to see how the docs align with what the SGIP is doing. Sometimes we receive contacts from other organizations outside of the SGIP asking for our opinion on what others are doing in the SG process.
- One item in the document is that the UK requires at least one reading per month whereas the US does not require this – even allows for opt-out processes in some states.
- Ken and Irene agreed to assist with the review.
- Please have something for the group within the next two weeks.

- Shodan search tool: Rebecca
- There has been talk of Shodan over the past two weeks. This website is able to reveal countless numbers of SCADA systems and in some cases make them wide open to hackers with the right tools. CSWG has been approached with this information and asked if they are addressing it. Utilities advise that they are blocking the information expressed in Shodan where found. It raises questions as to what can actually be searched online and the risks involved with protecting information from being found.

- Ken stated he believed this is not really a privacy issue; this is a security issue involving the web.
- Rebecca: Privacy and security overlap. If a search engine provides access to smart meter data, it could reveal personal activities or other types of personal information, making it a privacy issue.
- Ken was at ConnectivityWeek, there was also a meeting with IEC-program committee, project committee 118. Request from China and co-chairing with Dave Holmberg from NIST. EPRI and China's solution to hacking is to keep a physically separate network keeping them protected from the open web.
- Ward: This issue also came up during the Black Hat conference last year in conjunction with simple Google searches, regardless if the systems are password-protected or not. Oftentimes, especially in the control-system world, if access is granted, the user-credentials are set and not changeable. If there is something that is publicly available on the internet, you will be able to gain access either through the user or vendor's manual. For the last year, the security community has been trying to deal with how to better understand and protect the systems.
- ICS and the world – right now, there are quite a few publicly accessible search queries in Shodan for oil refinery companies. Even though companies know this fact, they will not take the systems offline because they are vested in the connectivity.
- Rebecca will put this topic on another agenda to be discussed in the future. She will pose more privacy-related questions regarding Shodan. It is an interesting topic.

- Privacy Use Cases – Christine: Making steady progress on going through the comments received and incorporating that feedback into the use cases document. No news other than they are coming along nicely.
- Training & Awareness – Rebecca: On hold until after the 3rd party recommendations paper is finished.
- PEV Team – Tanya: No new updates. Trying to getting work back from lead as to when they will be able to meet again.
- NSTIC – Amanda: On hold until pilot projects are released.
- 3rd party teams – Tanya standing in for Brent:
    - Two teams under 3rd party doing a lot of work.–
    - 3rd party recommendation paper –
        - Received a large number of comments and going through them all. We are more than halfway done. Starting meeting again next week on Friday.
        - Rebecca: Those meetings on the paper are permitting full-group participation. The final document resulting from these dedicated meetings will be the one passed to Marianne Swanson. If this is important to you, you need to give your input at these dedicated meetings before the final document is submitted.
        - Ken: Noticed there has been an issue with changing "shalls" to "should". Can we create a model regulation? Tanya advises no because it comes close to offering legal opinion and gets close to submitting regulation which is outside the group's scope. If PUC/PSC takes the document and adopts it, okay, but we cannot push them to do so.

- NAESB REQ 22 Team –
  - June 6th document is a draft report that Frances Cleveland and the standards subgroup will file with the SGIP that looks at the REQ 22 and compares/contrasts it to Vol 2 of the NISTIR and other high level security requirements found in other volumes. Over half of the report was completed by the standards group. We only drafted a small portion of the text but what we did contribute was significant. 1st table looks at high-level security controls in NISTIR and not found in REQ 22. The 2nd table is our comparison of what is in REQ 22 and how it stacks up with privacy recommendations within Vol 2 of the NISTIR. There are some things to know: We had at least one PUC rep and utilities rep and privacy rep. Still kept the group small enough to receive copies from NAESB on a temp basis. There is a very large difference in scope between the REQ 22 and the NISTIR. The NISTIR intends for the document to be applicable to everyone involved with SG. REQ 22 only deals with Distribution Companies releasing data to Third Parties. The scope difference left some pieces out that were referred to in the NISTIR. That is where "partially meets" comes into play and addresses the scope differences. There are a few actual gaps – particularly in things like the list of items recommended by NISTIR to be covered in policies and procedures (Use, retention, disposal of data). List in REQ 22 is not as comprehensive.
  - The second big table is something for everyone to look at. If you have the document, on the very last page, there are two sections of text and these we crafted. One is really a repeat of the other one. Recommendations are a repeat of the table information. First paragraph came from standards group and handles security. Second paragraph addresses privacy issues. Many people contributed to these recommendations. Glance through the table but definitely pay attention to the paragraph under 2.3.3/2nd paragraph. Standards group is asking for complete document ASAP because they have to review the information and pass it along to SGIP for further review.
  - What is the ultimate goal of this document? That goal is up to NAESB. These reports are seen as information because it is not seen as a glaring hole in guidelines. NAESB is not required to accept any part of the document because they are simply suggestions. The report will be published under the Twiki.
  - A second call can be scheduled if people have more to say. The deadline for calling Frances is Friday, June 15 at 1:00pm. If we're not finished by then, we need to be pretty close to being finished. Please also understand that the standard is not public information – it is copyrighted. The group cannot provide a copy of the standard if you would like to provide comments – you will have to obtain your own copy. We have asked to allow more people to review the standard but have not heard anything from NAESB to date.

  - Deadline for comments to Tanya: Open of business Monday, June 18th.

    - Tanya will hold a call sometime that week before Friday, June 22 to discuss the comments.

- Rebecca: Reminder that the SGIP 2.0 Business Sustainment Plan is available for review. It does involve some very significant changes. If you have comments, please submit them to the Twiki as soon as possible.

Next full group meeting is June 22nd at 11:00am EST.