

NIST 12.10.09 Smart Grid Privacy Subgroup meeting notes

Notes by Rebecca Herold

Please send distribution list any necessary corrections or additions!

Thanks to all of you participating and contributing in this group! I hope that all of you feel comfortable expressing your thoughts, concerns, ideas and suggestions about any privacy issues you see related to the smart grid. If we haven't talked about any of the specific privacy concerns you have, please let us know. We want to hear your opinions and feedback!

Next meeting: Thursday, December 17 at 11:00am est

Here are my notes from today's meeting:

- **Action Items**

- Send FINAL comments about NIST Smart Grid Framework document to Tanya **by 2:00pm est on 12/10/09: *Assigned - All***
- Send comments about the NISTIR 7628 privacy chapter comments received to the group for final discussion by end of day Tuesday 12/22: ***Assigned - All***
- For the responses to the NISTIR comments, create a boiler plate draft of language to point out that while we cannot create laws and regulations, but that the recommendations from NIST have historically been important for lawmakers to use when crafting laws and regulations: ***Assigned - Lillie***
- Provide links and documents about our group's discussions about personal information and PII: ***Assigned – Rebecca***
- Update and distribute proposed privacy best practices document to the group and post to twiki: ***Assigned – Rebecca***
- Over the next 4 weeks review the current draft of version 2 of the privacy chapter and other documentation gathered (such as in the spreadsheet, etc.) and identify what needs to be changed, added, corrected, etc throughout this time period: ***Assigned - All***

- **NISTIR 7628 Privacy Chapter V2**

- Next version needs to be done by mid-January, so much work needs to be going on now and through the next 4 or so weeks!
- Next version will:
 - Include and/or address issues that were within the PIA that were not included within v1 of the NISTIR 7628 privacy chapter
 - Add new material as we've been identifying and discussing
 - Address comments received for the privacy chapter of the first version of the NISTIR 7628

- **Frameworks document:**

- Discussed the Smart Grid Privacy Frameworks document (an approximately 2 page overview/summary of our group's work)
- Group members were given until 2pm est on 12/10 to send additional change suggestions to the group and for Tanya to use within the final version

- **Comments to NISTIR 7628 version 1 Privacy Chapter:**

- NIST's role is limited in what they can and cannot do with regard to creating standards, and making other types of authoritative statements.
- Historically it has been important for groups/agencies to comment on NISTIR documents because often lawmakers will take such documentation into consideration. Congress looks at NIST research and study documents and the associated recommendations when they are writing bills and regulations.
- Tanya: We do not want to put out responses to comments that are quasi-legal. For our type of group, NIST does not want to go on record as saying something should be a law. They can recommend best practices, and point out issues that must be addressed. Requested help for creating boiler-plate language. Lillie volunteered for this.
- We need to show within our next draft the value proposition of addressing privacy from a business standpoint. This is an opportunity to leverage the concept of trust and how organizations can then use it to promote privacy practices. Smart Grid possibilities are tremendous across the board.
- In general, with new services and technologies, many consumers assume security and privacy controls and protections are already built in. However, service providers and supporting vendors don't always see that as part of the bargain. Supporting privacy is an opportunity to differentiate a brand. Giving consumers more choice.
- We need to use consistent terminology throughout the privacy chapter and ensure the terms also are defined the same as within the other parts of the NISTIR. Important terms to include and consistently use include, but are not limited to, the following:
 - Consumers
 - Customers
 - End users
 - Perhaps using "premises" instead of "dwelling," "home" or "household" depending upon the use
 - Premises owner
- Benefits of PIAs; expand upon this in the next draft.
- Role based access: We had a detailed discussion on this. A few key concepts:
 - Work role or authorized process;
 - Access based upon Services, Operations and Payments;
 - Analyzing appropriate accesses should be part of the PIAs;
 - Give use cases and scenarios;
 - E.g., Similar to HIPAA and the exceptions to obtaining consents for each instance of Treatment, Payment and Operations;
 - E.g., GLBA arguments said the ATM processes would "break" if consents were necessary. It was dealt with through service provider requirements/exceptions;
 - If exceptions are written too broadly then they could go into other activities that the consumer did not really want.
 - The wording in any resulting standards, laws and regulations will be critical. Be specific about the issue and how it is worded and

implemented. Some situations can be addressed with exceptions, and some with contracting.

- How much data is necessary to perform the required activities?
Design the process to ensure that access to data is limited to only that which is necessary. This will be addressed in our verbiage.
- Should we create use cases? Yes! Need to list some.
- Lillie led discussion of her EPIC/CDT comparison document. Some points made:
 - Identification of unique devices and appliances: a completely new source and type of personal information.
 - Data flows will be used for new reasons.
 - Criminal interest in smart grid data
 - Notice and Choice: Tell people what is going on and what their rights are. How do you give choice? Don't tie notice and choice together?
 - Historically, in various fields, the distinction between product adoption/purchase and consent gets merged. The decision to sign up for power should be divorced from other decisions for information sharing. Making sure the decisions are very separate must be made clear.
- How to give people access to their smart grid data? What data is personal data? How can we make sure the data is understandable? With new types of personal information, how will we make consumers know what they are looking at? And how it is used?
- Following due process is not a guarantee that your information will be changed, but it spells out how you can pursue getting your information corrected/changed.
- Definition of PII; page 23 of CDT comments. Point to the personal information and PII discussions in our group from the previous weeks.
- End of December meetings:
 - Since there are major holidays that occur on the last two Fridays of December we will reschedule our meetings during those weeks from Thursday to Tuesday:
 - 12/22 meeting: 11am est
 - 12/29 meeting: 11am est