

1/27/12 – NIST Smart Grid Privacy Subgroup Meeting

Role Call

- Rebecca Herold – The Privacy Professor (Group Leader)
 - Eric Ackerman – EEI
 - Chris Paul – California Edison
 - Dan Friedman – Amdocs, Canada
 - Alex Churchill – Duke Energy
 - Di Ford
 - Ron Vader – DTE
 - John Hudson – Centerpoint
 - Steve Wright
 - Chris Villarreal – CPUC
 - Ike Collins
 - Dan Fredrickson - Tendril
 - Brent Struthers - Neustar
 - Ruth Yodaiken - FTC
 - Dan Francis – AEP
 - Carly Baker – OPOWER
 - Tanya Brewer – NIST (Group sponsor)
 - Mike Pagen
 - Krystina Schaefer – OH PUC
 - Amanda Stallings – OH PUC
 - Christine Hertzog – Smart Grid Library
 - Jules Polonetsky – Future of Privacy Forum
 - Aryeh Fishman – EEI
 - Dave Wollman - NIST
 - Marianne Swanson – NIST (CSWG Director)
 - Lee Aber - OPOWER
-
- Rebecca - Welcome New Members and Guests! Lately there has been confusion about the role of NIST and SGIP-CSWG groups. Today I am happy to have Marianne Swanson in attendance to describe the mission of our group.
 - Marianne – senior advisor for Information Technology Security at NIST and Chair of CSWG groups. Will provide discussion and description of groups.
 - Under EISA, NIST was mandated to help facilitate standards development – not to write them. Anything published is considered guidance and as a technical resource for standards development and/or policy if state or utility or vendor wants to take the information and use it to create their own policy. NIST’s broader role is to do exactly this – help others develop standards and/or policy. The organization is not a policy maker.
 - Examples: The NIST-IR 7628 is probably the best from the CSWG perspective. Organizations can take this document and implement it into their own standards.
 - Interoperability performance reference manual – that document is setting out a structure that can be used for a standards body to develop a certification program that can use this guide as an approach. Again – this is guidance.

- PAPS – providing technical resources material
 - PAP2 put out a NIST-IR on requirements
- Privacy group is doing the same thing – bringing good work together and bringing additional information to help others develop standards.
 - REQ 22 – it has requirements that are similar in nature that practices have.
- NIST is going to be reviewing under CSWG standards – REQ 22 against the NIST-IR high-level security requirements.
- If there is so much redundancy between recommended practices under NIST and REQ 22, why not do a mapping and point out gaps between the two documents. That could be a section in CSWG manual that can show what is missing on either side of the REQ 22 and CSWG standards.
- EEI has a concern that distinctions being drawn are going to be lost on policy makers and may cause confusion. There are already published documents that companies and policymakers are using that may duplicate what CSWG is doing. CSWG is not ANSI certified. Not as credible of a product. This is a concern.
- There is literally a treasure-trove of documents created by other organizations that are available from NIST under CSRC.NIST.GOV. These have been created for many years and are providing valuable services way beyond energy services. These guidance documents are of great value. Some are probably ANSI certified, but many are not, yet are still considered to be valuable resources for all types of organizations.
- We're not talking about technical cybersecurity at all – this is completely public policy.
- This is a group of very limited representation. We're talking about guidance – i.e. recommendation, developed by members of the group – not an ANSI certified process. Gives those who are ANSI certified great concern.
- If it's not an ANSI product, organization has a choice to use other resources and not the CSWG's resources. What's so bad about putting out a document that has been created by a group of people that is strictly guidance?
 - It may cause confusion – that's a potential problem. When there are potential conflicts and it's out there with all the other documents, it becomes problem-some.
 - There are all sorts of policies. This is strictly a policy document – not technical.
- No, this is NOT a policy document. It is recommended leading practices based upon gap analysis of existing documents and also with long-accepted international privacy principles.
- Remember that NARUC has taken note of NAESB product. This widely differs from NAESB product.
- The Privacy document applies to all entities using or benefitting from smart grid. There are a lot of vendors not under current regulations handling privacy-related data.
- Chris Villareal agrees with what Rebecca said and appreciates the efforts this group has put forth to harmonize national efforts and best practices.
- There were dozens of state laws taken into account when writing REQ 22.
- Company states that NAESB is the current standards board for utilities.
 - Third parties were not always jurisdictional. How does this document change any of that?
 - Who is going to oversee the 3rd parties is a separate issue.

- The NAESB effort, as Brent thought, dealt with utility data and not the data coming off the meter. This document created best practices for meter data, and didn't go back to NAESB because that's not the direction they were going.
 - This may not be the view of NAESB. We need clarification.
 - Clarification may be in the minutes from a while back.
 - Groups are more than welcome to contact NAESB for confirmation of agreement.
- Why is there such a resistance to this now?
 - Because companies thought they had done that with NAESB. Is the intent to fill a gap with customer-side of the meter or this an intent to influence standards?
 - Might get a little more consensus if this is limited to 3rd party vendors dealing directly with customers and leave utilities out of it.
 - REQ 22 was carefully focused on 3rd parties. There are recommendations for utility providers should do and that is the intent of that model.
 - Clarification:
 - A data minimization recommendation that implies that the utility needs to receive customer authorization to view their data. REQ 22 does not address a need for this. Line 168
 - We have this doc, have the draft NAESB standard.
 - Our CSWG document is best practices, it doesn't require anything, it is simply recommended privacy practices. Although there may be a possibility of states adopting this document. Already addressed in the NAESB, anything else is extra. Do we apply extra stuff to the utility or just the 3rd parties?
 - Question: Best practices recommendation, entities should limit the data they collect to only the services they have authorization for?
 - The implication of that statement is that the EDU has to specify that too. No one has ever challenged the need for data in the past. What is the right way to do this now?
 - Make a suggestion that NAESB address this issue.
 - Why haven't utilities been asked to review this document?
 - They have. All entities have been asked to participate in our group since mid-2009.
 - What is the concern with the concept of data minimization? It is a long-held international privacy principle. It will be noticeably absent to be omitted, and it is a significant privacy concept.
 - Standard to have a retail customer contract that the customer has agreed to.
 - This is a basic privacy principle. Why can't it be covered within the customer contract?
 - Certainly not a case for all jurisdictions that the utility operates in. There is a specific concern that customer authorization needs to be obtained by utilities. But the draft recommended privacy practices do not say this.
 - What about that statement needs to be changed? Authorization?
 - Consider customer buying energy through a tariff as needing authorization? Brent would.

- Some tariffs don't get that specific. No where is the customer asked permission to do anything. Can argue implied authorization, but authorization implies knowing.
 - In Cali, even before CPUC laws dealing with SG came out, utilities notified customers what their data will be used for.
 - This is a list of best practices according to whom?
 - Data minimization is an accepted international privacy principle.
 - Look at the top of the document, the very first line of the document doesn't address best practices, it states recommended privacy practices.
 - We are looking at privacy within the Smart Grid. To do that, we have to base it upon currently accepted privacy principles. This is not something new. This is something that all industries must address. It is covered in other regulations that data minimization is a best privacy principle.
 - Privacy principles are basic principles that apply to data that reveals information about individuals and consumers. They are not specific to only certain industries.
 - This might offer a solution: Looking at the data minimization line, what really is the sticking point is the authorization piece. What if it said as set forth in company's territory or tariff, if there is no authorization process, then there is nothing to cover?
 - If we limited this document only to the customer side of the meter, everyone would be happy?
 - If it's limited only to the customer side of the meter, than the electricity provider is not involved.
 - When the whole eco-system is discussed, what is covered is both entities receiving data directly from consumers, but also those who collect data from the utility.
 - Need to avoid competitive standards. Utilities did a lot of work with NAESB and that can be revised. We need to state this up front. Needs to be clear that this is not trying to be competitive with other standards already in place.
 - Some statements involved in the document conflict with company's current practices; some may even go against current standards already in place.
 - We can harmonize this with NAESB's cooperation – can create one standard that contains balance between all groups involved.
- Rebecca will meet with Marianne, Tanya and others and send out next steps to group when a suggested best plan forward has been established.
 - Next Meeting: February 10, 2012 at 11:00am EST.