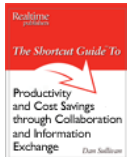


**Realtime community** "Leading the Conversation" **IT Compliance**

WE BLOG DIGITAL LIBRARY PODCAST Resident Editor: *Rebecca Herold*

**NOW AVAILABLE:**



« [HIPAA And Surveillance In Hospitals](#) | [Main](#) | [Smart Grid Privacy: Possible Privacy Standards To Address Concerns](#) »

**15 Smart Grid Privacy Concerns + Other Smart Grid Thoughts**

I've had about half a dozen folks ask me how things are going with the work I'm doing with the [NIST Smart Grid privacy group](#), and if I could provide an update since my last couple of posts on the topic [here](#) and [here](#).

The time is going by much too quickly, and I am getting a bit nervous as we get closer to when we need to have the next draft of the NISTIR ready, tentatively set for December 31; there is so much more to do in this **VOLUNTEER** group effort...

Here is a quick laundry list overview for some of the activities I've been doing within the group:

\* **Smart grid privacy concerns**

In October through our excellent Smart Grid privacy group meeting discussions I expanded the possible smart grid privacy concerns list to 15. See my updated PDF, "[Smart Grid Privacy Concerns: October 2009](#)" at [http://www.privacyguidance.com/files/SmartGrid\\_PrivacyHeroldOct2009.pdf](http://www.privacyguidance.com/files/SmartGrid_PrivacyHeroldOct2009.pdf)

\* **Smart Grid Privacy Standards**

We've been discussing and addressing the need to create some actual privacy standards for the organizations that are part of the smart grid to follow. NIST indicates they've been working with the ISO/IEC folks to create some privacy standards, but since those are not yet publicly available, and I've not been able to see them, I created the following first DRAFT proposed privacy standards for organizations that are part of the smart grid (and beyond) based upon long-established privacy principles (from the OECD and then subsequently another draft from AICPA/CICA), as well as existing data protection laws and regulations as I've documented within the NIST smart grid privacy group working spreadsheet:

- 1. Consent & Choice:** The organization must describe the choices available to individuals and obtain explicit consent if possible, or implied consent when this is not feasible, with respect to the collection, use and disclosure of their personal information.
- 2. Notice & Purpose Specification:** The organizations must provide a clearly worded notice, at or before the time of collection, describing the purpose for the collection, use, retention, and sharing of personal information, along with listing the items that are collected.
- 3. Individual Participation & Access:** Organizations must provide a process for individuals and households to allow them to ask to see their corresponding personal information. Organizations must also provide a process to allow individuals and households to request the correction of perceived inaccuracies within the corresponding personal information provided by each organization. Individuals and households must also be informed about all the other parties with whom their corresponding personal information has been shared.
- 4. Data Quality/Integrity/ Accuracy:** Organizations must make every effort, using documented policies, procedures, standards and ongoing training and awareness communications, to ensure that personal information and other data collected from smart meters is accurate, complete and relevant for the purposes identified in the notice, and remains accurate throughout the life of the information within the control of the organization. Policies and procedures must be in place to notify all other entities when corrections to personal information is made so that they can appropriate correct the corresponding information for which they are the custodians.
- 5. Use Limitation:** Information within the smart grid networks and systems should only be used or disclosed for the purpose for which it was collected and should only be divulged to those parties authorized to receive it. Personal information should be aggregated or anonymized wherever possible to limit the potential for computer matching and data mining the records.
- 6. Retention & Disposal Policies/Practices:** Smart meter information and corresponding personal information should only be kept as long as is necessary to fulfill the purposes for which it was collected. When it is no longer needed for the

**SEARCH**

**MOST ACTIVE POSTS**

- » [15 Smart Grid Privacy Concerns + Other Smart Grid Thoughts](#) **comments (1)**
- » [10 Smart Grid Consumer-to-Utility Privacy Concerns; Are There More?](#) **comments (2)**
- » [CEs and BAs: Be HIPAA/HITECH Compliant Or Pay A Hefty Penalty](#) **comments (2)**

**LIBRARY RESOURCES**

- » [Realtime Essentials Series](#)
- » [Realtime eBooks](#)
- » [Rebecca's Upcoming Speaking Dates](#)

**FEATURED RESOURCES:**



**REALTIME COMMUNITIES**

- » [Messaging and Web Security](#)
- » [Unified Communications](#)
- » [Vista](#)
- » [Windows Server](#)

**NEWSLETTER**

Email Address:

**MONTHLY ARCHIVES**

- » [November 2009](#)
- » [October 2009](#)
- » [September 2009](#)
- » [August 2009](#)
- » [July 2009](#)
- » [June 2009](#)
- » [Complete Archive](#)

**RSS**

- » [FEEDBURNER](#)
- » [PODCAST](#)
- » [iTUNES](#)

**ASK THE EXPERT**

Have a question for our resident expert? [Email your questions to Rebecca.](#)

**10 MODULES**

**5 WEEKS 5 EMAILS**

**PCI COMPLIANCE BOOTCAMP**

**QUALYS**  
ON DEMAND SECURITY

**RECENT POSTS**

- » [Smart Grid Privacy: Possible Privacy Standards To Address Concerns](#)
- » [15 Smart Grid Privacy Concerns + Other Smart Grid Thoughts](#)
- » [HIPAA And Surveillance In Hospitals](#)
- » [CEs and BAs: Be HIPAA/HITECH Compliant Or Pay A Hefty Penalty](#)
- » [Smart Grid Privacy: Laws and Implications](#)
- » [6 Critical Factors for Effective Information Security & Privacy Policies](#)
- » [Who Are Your Business Associates?](#)
- » [HIPAA/HITECH Etc. Retention: Does Your Reality = Your Requirements?](#)
- » [Proposed HIPAA Privacy Rule Change Explicitly Makes Genetic Info PHI](#)
- » [Privacy For The Deceased](#)

**CATEGORIES**

- » [Government](#)
- » [Identity theft](#)
- » [Information Security](#)
- » [Laws & Regulations](#)
- » [Lost & Stolen Laptops](#)

stated purposes for which it was collected, it should be irreversibly be deleted/destroyed using disposal method which, at a minimum, meets NIST disposal standards.

7. **Transparency & Openness:** Documented privacy policies must be made available to individuals and households that are part of the smart grid systems and networks. Individuals and households must be given the ability and process to challenge an organization's compliance with their stated privacy policies as well as their actual privacy practices.

8. **Collection Limitation:** Only information that is required to fulfill the stated purpose(s) should be collected from individuals from households. Organizations collecting information must follow fair information processing practices. Personal information must be collected directly from each individual for household, their corresponding smart meter, or an approved mobile smart meter data collection device, unless there are approved and documented reasons why this is not possible.

9. **Security/Safeguards:** Organizations that are part of the smart meter network must protect personal information, in all forms, from loss, theft and must prevent unauthorized access, disclosure, copying, use or modification.

10. **Accountability & Management:** Each organization must formally appoint a position, team, department or individual to ensure that information security and privacy policies and practices exist and are followed. Documented requirements for regular training and ongoing awareness activities must exist and be consistently followed.

11. **Disclosure and Limiting Sharing:** Personal information must be used only for the purposes for which it was collected. Personal information must not be disclosed to any other parties except for those identified in the notice, or with the explicit consent of the corresponding individual or appropriate household representative.

12. **Monitoring & Enforcement:** Each organization that is part of the smart grid network and systems must monitor compliance with its privacy policies and procedures and have procedures to address privacy-related inquiries and disputes. Audit functions must be present to monitor all smart grid data and personal information uses, sharing and modifications.

#### \* **Proposed certification recommendations**

Wouldn't it be a good idea to have privacy certifications for not only the organizations that are part of the large smart grid, but also for the smart meters to help ensure they are appropriately addressing privacy and providing households with informed decision-making capabilities for how the information collected from their homes through these devices are used? I think so. If you don't, please let me know why.

I believe the following would be two beneficial types of certifications to require for entities that make up the smart grid:

1. **Organization privacy self-certification** (for smart grid, but could be a way to "certify" any organization in any industry; follows along the concept of the EU Safe Harbor program):

With wording similar to the following: "We strongly recommend the energy industry follow the lead of the U.S. government agencies who perform annual privacy impact assessments (PIAs) and require each organization that participates in the smart grid network and systems, as well as each organization that performs activities for such organizations, to:

- 1) perform an annual PIA, provide it to each state's energy commissioner office to review, and
- 2) perform a PIA on each new system, network, or smart grid application and provide it to each state's energy commissioner office to review.

The state energy commissioner office will:

- 1) either acknowledge the PIA is appropriate and send approval to the organization, after which the organization will post it on their website, or
- 2) notify the organization and communicate the privacy deficiencies identified within the PIA and ask them to correct them. While the correction is being made, a notice containing an executive summary of the PIA findings must be posted on the organization's website, along with a high-level description of the corrective actions being performed and corresponding target dates for completion."

2. **Smart Meter device privacy certification:**

With wording similar to the following: "We strongly recommend that the energy industry require each smart grid meter be reviewed by prior to its use and implementation, and be certified as appropriately providing privacy choices and having proper privacy protections. "

#### \* **Definitions**

Working on creating definitions for the privacy portion of the NISTIP for terms

- » [Miscellaneous](#)
- » [Non-compliance Sanctions Examples](#)
- » [Podcast](#)
- » [Privacy Incidents](#)
- » [Privacy and Compliance](#)
- » [Training & awareness](#)

#### REBECCA HEROLD'S BIO:

Rebecca Herold, CISSP, CIPP, CISM, CISA, FLMI, has been providing information security, privacy and regulatory assistance and services to organizations from a wide range of industries for the past two decades. Rebecca was instrumental in building the information security and privacy program while at Principal Financial Group, which was awarded the CSI Information Security Program of the Year Award in 1998. IT Security ranked Rebecca as one of the top 59 IT security influencers, and Computerworld put Rebecca their list of the world's best privacy experts and on their list of the best privacy consulting firms in both 2007 and 2008. Rebecca has been CPO for two consulting organizations, and has had her own information privacy, security and compliance business since 2004. Rebecca has written chapters for several books, dozens of articles, and has been writing a monthly privacy column for the CSI Alert newsletter since the beginning of 2001, and is working on her 13th book. Some of her other books include The Privacy Papers, Managing an Information Security and Privacy Awareness and Training Program, The Definitive Guide to Security Inside the Perimeter (Realtime Publishers), The Shortcut Guide to Improving IT Service Support through ITIL (Realtime Publishers), and The Practical Guide to HIPAA Privacy and Security Compliance. In addition, Rebecca is the leader of The Realtime IT Compliance Community where she posts to her IT Compliance weblog. You can contact Rebecca at: [rebecca\\_herold@realtimepublishers.net](mailto:rebecca_herold@realtimepublishers.net).

were working on creating definitions for the privacy portion of the NIST IR for terms such as "personal information," "personally identifiable information," "multi-part personal information" and so on.

**\*  Laws, regulations and standards that may cover the smart grid activities and data**

The short, and incomplete, list includes some of the most far-reaching laws/regs/standards:

- OECD Privacy Principles  
([http://www.oecd.org/document/18/0,2340,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_](http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_))
- AICPA Generally Accepted Privacy Principles  
([http://infotech.aicpa.org/NR/rdonlyres/0AB737BF-55D1-459B-ADD5-179A270E863C/14379/GAPP\\_PRAC\\_0909.pdf](http://infotech.aicpa.org/NR/rdonlyres/0AB737BF-55D1-459B-ADD5-179A270E863C/14379/GAPP_PRAC_0909.pdf))
- FTC Marketing Guidelines (February 2009)  
(<http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>)
- Canada's PIPEDA (<http://laws.justice.gc.ca/en/showdoc/cs/P-8.6/sc:1/en#anchors:1>)
- EU Data Protection Directive (<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>)
- HIPAA  
(<http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacypolicy/adminsimpl>)
- GLBA (<http://www.ftc.gov/privacy/glbact/glbsub1.htm#6802>)

We probably don't need an exhaustive list, but these are significant. We are identifying other significant ones to add that are important for the purposes of the next draft of the NISTIR.

**\*  State level activities**

We are considering the activities and information from each of the states for what their energy and utilities commissions have done to date with regard to researching and/or addressing the privacy issues within the smart grid components. We will hopefully be getting information from the NARUC conference that we can add to the NISTIR.

***It is important to point out that the above are just suggestions and ideas being discussed within our NIST smart grid privacy group, and are not necessarily going to be included in the next draft of the NISTIR. They should also NOT be considered as being the viewpoints of NIST!***

Do you have any comments, concerns, or other information to add to the above? I welcome all thoughts and input!

Tags: [awareness and training](#) [information security](#) [IT compliance](#) [IT training](#) [NIST](#) [personally identifiable information](#) [PIA](#) [PII](#) [policies and procedures](#) [privacy impact assessment](#) [privacy law](#) [privacy training](#) [security training](#) [Smart Grid](#) [Smart Meter](#) [SmartGrid](#)



Posted by Rebecca Herold on November 9, 2009 5:12 PM | [Permalink](#)

**TrackBack**

TrackBack URL for this entry:  
<http://www.realtime-itcompliance.com/type/mt-tb.cgi/1051>

**Comments**

In response to an Article in local Newspaper Power Dreams? article dated August 25, 2009: (Press Enterprise Riverside CA)

Why build the new transmission lines? Why build Solar Electric Generating plants so far from where it is going to be used? What is wrong with the existing system that we have now?

The answer is simple, because we are over thinking the solution. We can install smaller solar farms within the communities and utilize private and public land. For instance the PPA programs that cities are looking into and implementing is a great start. Allowing private companies to put out the upfront cost of building the system while the company is reaping the profits in the long run, this is a win-win situation for both sides.

By utilizing Solade Concepts, Solar Structures (Solar Bus Stop, Comfort Station, Cahana Umbrella and more) throughout the cities, factories or businesses, they

■ Cabana, Umbrella and more) throughout the cities, factories or businesses, they can be placed in parking lots, (To Charge Electric Vehicles) sidewalks, eating areas, around pools or anywhere the need arises, while building an internal and virtually invisible solar farm. Residential use could also be part of the solution by adding a multi-functional structure at a home as opposed to a large, costly rooftop project. This concept will allow the renewable electricity to be used where the actual electricity is being generated as opposed to the massive transmission lines project. This type of undertaking may not solve the entire problem but it sure will take a big bite out of it.

If these plans are implemented it will keep utility rates down as the utility companies will not have to build new plants, transmission lines or smart grids, lowering the operating cost of their company.

There is an issue of what about low sun light or cloudy days. I was thinking more about that comment about of how we get the energy when there is no sun. I think that the storage systems could be placed in areas where they use the energy. For instance, a building having a backup generator room or a house with a water heater closet they also could have a electricity battery storage room. Then still allowing the solar energy to be generated at a different location ( landfill). The remote location still could be producing the energy but the actual users will store it for low sun time or cloudy days. This may work with all the advancements in battery technology. I know this will be hard to implement but it is a idea. It will take time to build any kind of renewable energy grid but if we start now putting these ideas out there it may just become a standard

I like to call it the Micro Grid.

Posted by: [Andrew Ferrick](#) | [November 10, 2009 6:10 PM](#)

**Post a comment**

All comments are approved by site leader before appearing here. Thanks for commenting!

Name:

Email Address:

JRL:

Remember personal info?

Comments: (you may use HTML tags for style)

▲  
▼

[CONTACT US](#) | [PRIVACY POLICY](#) | [FAQ](#) | [ABOUT US](#) | [TERMS OF USE](#)