



This slide set is being provided to serve as a starting point for those within Public Utilities or Services Commissions to help them effectively and efficiently plan for their own internal information security and privacy education program as it relates to Smart Grid privacy. These slides will provide information as a way to help “train the trainer.”

These slides are meant to cover Public Service Commissions as well as Public Utilities Commissions, even though PSCs are not specifically called out in every instance.

We’ve provided significant additional information within the speaker notes that you may wish to use when you deliver your own, tailored training. Please be sure to add any other information to your training as it pertains to your own organization’s unique and specific needs. For example, you may want to point to specific organization privacy or security policies associated with some of the slides. You could also include examples of incidents or situations that have actually happened either within your own organization, or as reported in the news, that are related to information on specific slides.

Addressing privacy concerns up front is better than waiting until after consumers or employees complain. It helps to be prepared by knowing the basics of privacy, and also how to accurately provide an overview of how privacy should be protected within organizations whenever vendor, utilities, or consumers may ask.

SGIP-CSWG Overview

2

- SGIP
- CSWG
- Disclaimer:
These slides were created by the CSWG Smart Grid Privacy group to provide a tool for organizations involved with the Smart Grid to use to help facilitate training and awareness about Smart Grid privacy issues and risks. These slides are not endorsed by NIST, nor are they required to be used under any existing law or regulation. They are also not intended to be considered as legal advice.



SGIP – Initiated by the National Institute of Standards and Technology (NIST), the Smart Grid Interoperability Panel (SGIP) plays a leadership role in facilitating and developing the essential components of the Smart Grid (as conceived in the Energy Independence and Security Act of 2007) and in realizing the national policy for the transformation of the power system to the Smart Grid.

CSWG - The Cyber-Security Working Group is a standing working group under the SGIP.

Disclaimer – These slides were created by the CSWG Smart Grid Privacy group to provide a tool for organization involved with the Smart Grid to use to help facilitate training and awareness about Smart Grid privacy issues and risks. These slides are not endorsed by NIST, nor are they required to be used under any existing law or regulation. This is not intended to be considered as legal advice.

The Purpose

To address privacy issues related to consumer adoption of Smart Grid technologies

- Understanding what information may be collected
- Limiting the data collected to only that necessary for delivering and billing for services
- Describing why information is collected
- Explaining how information is used
- Knowing how to securely store the information
- Knowing who has access to this information
- Establishing information retention and disposal standards
- Determining how to inform customers and utilities about these practices



Training should cover not only privacy within PUCs/PSCs, but also access within the collector organization as well as within the third party.

With regard to the 2nd bullet point, "limiting the data collected to only that necessary for delivering and billing for services," it is important to note that this is related to the 6th bullet point "knowing who has access to this information" because everything becomes more complicated if 3rd parties (e.g., OPower) possibly are granted access to data over time due to their involvement with energy saving strategies for customers. These points combined possibly allude to utilities retaining data for other reasons beyond system operation and billing disputes (namely, history of energy use when customer energy saving strategies are activated by 3rd parties contingent upon states' jurisdictional powers).

Utilities and other entities possessing energy usage data should retain data only as long as needed for system operation and billing disputes.

Utilities and other entities possessing energy usage data should not use data for any purpose not communicated to, and where possibly explicitly agreed by, the customer. This concept of providing notice and obtaining consent should also apply to sharing data as well.

Our Objective

To help promote effective privacy training and awareness communications and activities for all participants within the Smart Grid and provide tools to support this objective that will also document the:

- Topics that should be covered
- Training/Awareness possibilities
- Possible communication methods

The logo for SGiP (Smart Grid Information Privacy) is located in the bottom right corner of the slide. It features the letters 'SGiP' in a stylized green font, with a circular graphic element behind the 'i' and 'P' that contains icons representing a smart grid and privacy.

This slide set is provided to assist those with awareness and training responsibilities within PUCs to know and understand the privacy issues involved within the smart grid, and then create awareness and training materials for their own organizations to cover these issues. These slides serve as a **starting point** for PUCs, and are not meant to be legally binding directives. They are to provide direction and to help facilitate creative thinking for effective regular training and ongoing awareness communications within PUCs.

The Audiences

- Users of Smart Grid technologies vary from utility companies to consumers to government and vendors. Each requires a unique approach and message regarding privacy for information related to Smart Grid technologies.
- There are many types of audiences involved.



When giving training using these slides be sure to provide and describe, ideally verbally but also possibly as a handout or an additional slide, the following list of audiences that are involved within the Smart Grid:

- Utilities
- Entities contracted by utilities: These are companies that represent themselves as being the utilities even though they aren't. For instance ITRON makes the smart meters themselves, and they often speak directly with the consumers on behalf of the utilities. Another example, OPOWER is sending information directly to consumers but it looks like it came from the utility.
- Third parties doing work for utilities. These would be companies that do work for the utilities, and do not represent themselves as speaking on behalf of the utilities. For examples, IT companies, such as IBM, that are updating servers involved within the smart grid, but are not doing that work as the utility itself.
- Consumers
- Entities contracted directly by consumers (contingent upon each state's jurisdictional powers)
- PUCs/PSCs
- Smart Grid technology vendors (i.e., meters, appliances) (contingent upon each state's jurisdictional powers)
- Lawmakers and other government agencies

Or, if you prefer, you can put the list on this slide. We put it in the speaker notes to create space and allow for PUCs to add their own images to the slides, if they'd like to do this.

Public Utility Commissions (PUCs)

6

Information gathered that should be covered by training and awareness messages

- Personal information
- Energy usage
- Location enabled technologies (e.g., GPS coordinates)
- Smart Meter identifiers (e.g., AMI IP address)
- Consumer home area network (HAN) / energy management systems and associated data
- Plug-in Electric Vehicle (PEV) data
- Add other and future topics as needed



Awareness and training activities should center around PUCs' already-established rules and regulations as well as generally accepted business practices and/or privacy principles. Programs should be updated as regulations and practices change within the industry.

To ensure a baseline understanding of personal information, PUCs should have training in place covering the types of personal information (including account numbers) and then discuss the types of information that clearly is, or could be, personal information that may be handled by utilities or other entities under their jurisdiction.

A HAN is a type of residential LAN.

PUCs can include examples and suggestions for each of these items, as appropriate for their particular offices.

PUCs should be aware of the data that is available or accessible from PEVs.

Third party contracts might include data items that should be included on this slide.

Topics for PUCs

7

PUCs should cover a wide range of topics to ensure employees and consumers understand the impact, as well as how they may impact the utility companies.

1. ***Basic privacy principles*** *
2. ***Identifying privacy impacting data*** *
3. ***How to safeguard data*** *
4. ***Applicable laws and regulations*** *
5. ***Policies and procedures that include coverage of Smart Grid technologies*** *
6. ***Educating consumers about utility privacy practices*** *
7. ***Obligations of other entities third party and contracting agents*** *
8. Data breach notice practices
9. Responding to consumer inquiries about privacy
10. Privacy impact assessment requirements and instruction
11. Other topics applicable to PUC territory

* These are necessary for all PUCs



PUCs should adjust this list as it applies to their state and other applicable requirements.

The topics depicted bold italicized font generally apply to all PUCs/PSCs.

Related to item #2, PUCs need to be aware that detailed consumption data can infer detailed customer activities unrelated to energy delivery. Negative effects of data archiving beyond that essential for energy delivery and system operation could result in:

- Involving the service provider in civil suits.
- Making the service provider an arm of the police.
- Discouraging customers from participating in smart grid projects as word of these secondary effects becomes known.
- Casting the service provider in the role of "Big Brother."

In particular for item #5, privacy policies should be established before technologies are deployed as is being done in some European countries.

In particular for item #6, PUCs should encourage utilities to establish consistent ways of informing consumers about, and providing them with some control of, the personal data collected about them, and the energy usage data collected from them.

In particular for item #8, PUCs need to determine what, if any, data breach laws or regulatory requirements exist for their state and then provide training as appropriate based upon their requirements.

Laws and regulations are constantly changing, so it is important to keep these topics up to date. These may include not only federal, but also state and local level regulations.

Training Possibilities for PUCs

Each PUC can choose the best training method and vehicle for its work environment. The following are some of the methods that are good to consider:

- Online training modules (produced in-house or outside of the organization)
- Webinars
- In-house training provided by staff, utilities, or 3rd party
- Videos
- Seminars/Conferences
- Other training activities
- See more ideas within SP 800-50 "Building an Information Technology Security Awareness and Training Program" at <http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf>



Consider making training for Smart Grid privacy mandatory for all employees who access smart meter data, answer questions about smart meter data or consumer privacy issues, as well as those employees who have direct contact with the public and with customers. Employees not only need to understand privacy basics, but they also need to be able to know how to speak with the public about jurisdictional privacy practices.

Provide awareness communications and activities on an ongoing basis. Training should be conducted on a regular basis with communication regarding new policies as they become applicable. When a PUC is introducing smart grid privacy concepts for the first time, training should be given immediately. If the state PUC uses an intranet page for internal communications, a link should be dedicated for employees to review training materials and smart grid policies.

Also, track training attendance and awareness communications distributions. You need to make sure your employees are participating if your training is going to be effective.

Awareness Possibilities for PUCs

Each PUC can choose the best communication method for its work environment and culture. This is limited only by your own imagination.

- Websites (internal or external)
- Social media sites
- Radio/TV
- Print (i.e., magazines, newspaper, posters)
- Focus groups
- Email
- Podcasts
- Whitepapers
- Libraries
- Professional associations
- And others specific to each PUC



Awareness possibilities are limited only by your imagination. Provide awareness communications and activities on an ongoing basis. Monthly at a minimum, weekly preferred for the beginning of an awareness and training program where you are just introducing the concepts of smart grid privacy.

When giving training be sure to provide, verbally, the following list of possibilities:

- Websites (internal or external)
- Social media sites
- Radio/TV
- Print (i.e., magazines, newspaper, posters)
- Focus groups
- Email
- Podcasts
- Whitepapers
- Libraries
- Professional associations
- And others specific to each PUC

Or, if you'd prefer the list over the images, put them on the slide.

Fair Use Exceptions: Provide information about how this applies to your organization.

Groups to Deliver Education

10

Depending on the targeted audience (external or internal), the individuals or groups that deliver the training and awareness messages can impact the overall acceptance of the message. Here are groups that have expertise in privacy and may be able to provide resources and/or assistance for training activities and/or awareness communications:

- Representative from within a utility
- PUC training areas
- Third party training vendors with expertise in this topic
- Government agencies (e.g., DoE, NIST)
- FTC for general consumer privacy information
- GridWise Architecture Council (GWAC)
- National Association of State Utility Consumer Advocates (NASUCA)
- Smart Grid Interoperability Panel (SGIP) CyberSecurity Working Group (CSWG)
- National Initiative for Cybersecurity Education (NICE)
- Federal Information Systems Security Educators' Association (FISSEA)
- North American Energy Standards Board (NAESB)
- Consumer groups



- NICE: <http://csrc.nist.gov/nice/> Email contact: nice.nist@nist.gov
- SGIP: <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WebHome> Email contact: sgip.administrator@enernex.com
- CSWG: <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG> Email contact: marianne.swanson@nist.gov
- CSWG privacy subgroup: <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGPrivacy> Email contacts: rebeccaherold@rebeccaherold.com; tanya.brewer@nist.gov
- FTC privacy guidance includes: <http://business.ftc.gov/privacy-and-security>
- NASUCA: <http://www.nasuca.org> Email contact: nasuca@nasuca.org
- NAESB: <http://naesb.org/> Email contact: naesb@naesb.org
- GWAC: <http://www.gridwiseac.org/> Email contact: gridwiseac.coordinator@pnl.gov