Smart Grid Standards: Implications for State Regulatory Commissions

Background and Frequently Asked Questions

prepared for

FERC/NARUC Collaborative on Smart Response

prepared by

Roger Levy, Charles Goldman and Chris Hickman[1]
Lawrence Berkeley National Laboratory

NARUC Annual Meeting
Atlanta GA

November 2010

[1] LBNL provides technical support and assistance to the FERC/NARUC Smart Response Collaborative on Smart Grid implementation issues with funding from Department of Energy Office of Electricity Delivery and Energy Reliability). Roger Levy and Chris Hickman are consultants to LBNL.

List of Acronyms and Abbreviations

AMI	**Advanced Metering Infrastructure**
ANSI	**American National Standards Institute**
CIM	**Common Information Model**
DOE	**Department of Energy**
EISA	**Energy Infrastructure and Security Act of 2007**
EPRI	**Electric Power Research Institute**
FAQ	**Frequently Asked Question**
FCC	**Federal Communications Commission**
FERC	**Federal Energy Regulatory Commission**
FPA	**Federal Power Act**
GWAC	**Gridwise Architecture Council**
IEC	**International Electrotechnical Commission**
IEEE	**Institute of Electronic and Electrical Engineers**
ISO	**Independent Standards Organization**
IT	**Information Technology**
LBNL	**Lawrence Berkeley National Laboratory**
NAESB	**North American Energy Standards Board**
NARUC	**National Association of Regulatory Utility Commissioners**
NEMA	**National Electrical Manufacturers Association**
NERC	**North American Electric Reliability Corporation**
NIST	**National Institute of Standards and Technology**
OASIS	**Organization for the Advancement of Structured Information Standards**
OMB	**Office of Management and Budget**
PAP	**Priority Action Plan**
RAP	**Regulatory Assistance Project**
SAE	**Society of Automotive Engineers**
SDO	**Standards Development Organization**
SGIP	**Smart Grid Interoperability Panel**
SRS	**System Requirements Specifications**
T&D	**Transmission and Distribution**
W3C	**World Wide Web Consortium**

Introduction

This LBNL document focuses on national smart grid interoperability standards (*standards*) being coordinated by NIST. This document is intended to address two objectives. Section 1 provides background on the EISA[2] directive[3] that NIST coordinate development of *standards*. Information is presented to describe the types of *standards* being introduced, why they are necessary, and how they may affect state regulatory commissions, utilities and customers. Section 2 provides an FAQ framework for reviewing and assessing the impacts and concerns related to each of the specific *standards*. We use this FAQ framework to review the first five *standards* that NIST now considers ready for review by the FERC.

Section 1. A Brief Overview of Smart Grid Standards

EISA outlined a statement of support for development of a smart grid that included ten objectives for modernizing the infrastructure and operation of the electric grid. A key EISA assumption is that a modernized smart grid will substantially expand the use of digital, automated information and controls together with new technologies to improve system reliability, interoperability, and expanded customer service options. To make certain that these components work together, one of the ten EISA objectives calls for the development of new *standards* to guide the integration of expanded information flows with the anticipated new supply and demand technologies, specifically:

> <u>EISA SEC. 1301.</u> [4]
>
> 9. *Development of standards for communication and interoperability[5] of appliances and equipment connected to the electric grid, including the infrastructure serving the grid.*

The remainder of this section provides background information to provide the context for understanding and evaluating specific smart grid standards.

1. <u>Why are *standards* important to smart grid development?</u>

Smart grid represents the end-to-end integration of bulk generation, T&D, distributed generation, and customer systems overlaid with sensors and connected with multiple information and communication systems. Smart grid is expected to use digital information, automation, communication, and a high level of system integration to modernize the electric grid.

All these pieces need to be able to communicate with one another. If all hardware and information systems were supplied by a single vendor, there would be a very high probability that all of the pieces would connect and exchange whatever information they need to work properly. In a scenario that includes multiple suppliers that want to provide equipment or information systems, there has to be some sort of standard or interface that enables the systems to work together. Generally, standards are developed through the iterations that lead to a dominant vendor or technology that defines a de

---

[2] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h6enr.txt.pdf

[3] EISA sec. 1305(a). The Institute's primary function with regard to smart grid is to be a coordinator for the variety of smart grid standards development initiatives.

[4] EISA sec. 1301

[5] Docket No. PL09-4-000, 126 FERC 61,253, 18 CFR Part Chapter 1, Proposed Policy Statement and Action Plan, March 19, 2009. Interoperability is defined as: The ability of systems or products to work with other systems or products without special effort by the customer.

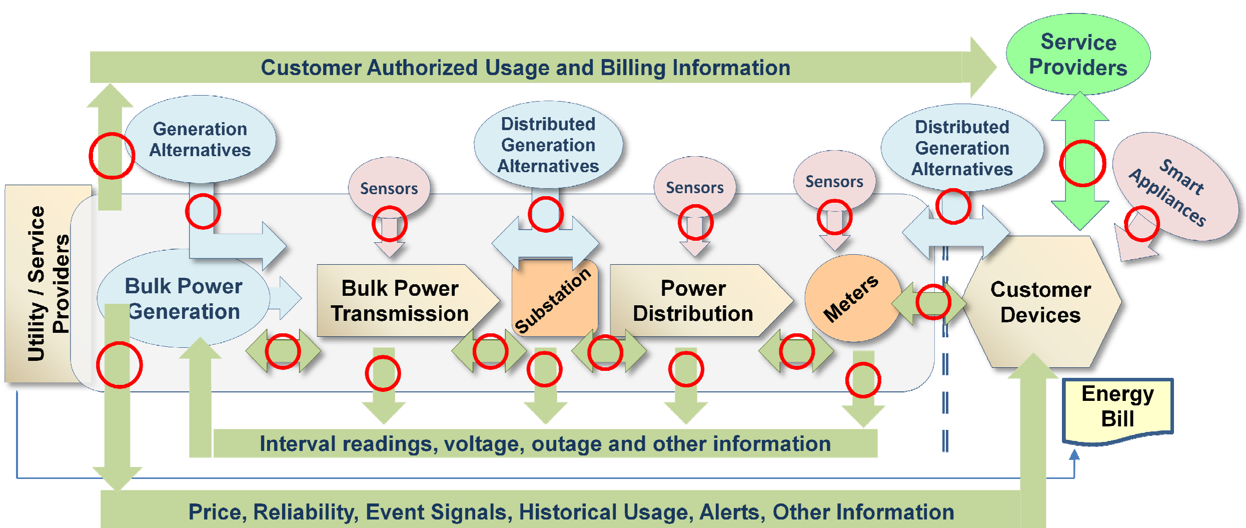
facto standard (*e.g.* DVD and BlueRay). If there was a single provider or a de facto standard that had emerged, then a separate standards setting process would be unnecessary.

The electric grid, however, is supported by multiple suppliers and vendors. Multiple suppliers reduce the risks associated with dependence on a single supplier. Competition among suppliers provides a more reliable supply chain, lowers costs, and increases potential innovation benefits. Systems with multiple suppliers require standards to better define how all of the hardware and information pieces connect.

Standards generally are developed to address the interfaces or interconnections between two components of a system. Interfaces can be translated into software or hardware requirements.

Figure 1 provides a simplified schematic of the smart grid vision, where the red circles identify some of the many interfaces or interconnection points between various elements of the electric grid. For example, standard revenue meters installed on a customer premise currently adhere to both hardware and software standards: (1) a standard socket design, ANSI C12.7[6], assures that all qualified vendor meter products are plug-compatible and interchangeable, and; (2) a software standard, ANSI C12.19[7], defines a table structure to standardize the data collected from and passed between the meter and the utility data collection system. Both standards reduce meter costs by increasing the compatibility between competitive vendor products. These standards also reduce the costs of data collection by making data transfer between competing vendor products transparent to the utility data collection system. Many of the new smart meters will be subject to additional standards to guide communications, data exchanges, and security between the meter and customer in-home displays, control devices, and third-party service providers.

Figure 1. Smart Grid Schematic – Interfaces and Interconnection Points.



Standards eliminate incompatibilities between vendor products and simplify testing, implementation, system security, maintenance, and development of monitoring and operational practices necessary to manage grid resources. Standards also:

---

[6] Requirements for Watt-hour Meter Sockets, American National Standards Institute, Revision of ANSI C12.7-1993, April 15, 2005, http://www.nema.org/stds/complimentary-docs/upload/C12.7.pdf

[7] http://www.nema.org/media/pr/20090326a.cfm

- Establish technical specifications to achieve the required level of compatibility, interchangeability, or commonality to obtain interoperability between system components and systems;
- Establish a common perception and understanding of system operations;
- Provide data compatibility and eliminate data incompatibilities; and
- Facilitate collaboration between units within an organization and between organizations, which facilitates system interoperability.

2. **What types of smart grid *standards* will be introduced?**

A 'Roadmap Report'[8] published by NIST in September 2009, developed a reference model to identify 77 existing or in-development *standards* that can be used to support smart grid. NIST has focused development efforts on eight areas prioritized by FERC in a Smart Grid Policy Statement[9] and stakeholder input. The priority areas include:[10]

- Demand Response and Consumer Energy Efficiency
- Wide Area Situational Awareness
- Electric Storage
- Electric Transportation
- Advanced Metering Infrastructure
- Distribution Grid Management
- Cyber Security
- Network Communications.

Through a series of workshops, NIST identified 16 initial existing *standards*, later expanded to 17 (see Table 1). These standards appeared to have strong stakeholder consensus. These standards have wide industry support, have been proven in practice, and provide useful guidance for the Smart Grid. This list was expanded to 31 *standards* based on public comments and additional analysis. Based on input from public workshops NIST determined that many of the *standards* on their initial list required revisions to address smart grid requirements and that several new *standards* were required to fill gaps between existing *standards*. NIST used the combination of the 31 identified standards and the associated gaps to prioritize standards and issues for immediate resolution. "Among the criteria for inclusion on this initial list of 17 standards were: 1) immediacy of need, 2) relevance to high-priority Smart Grid functionalities, 3) availability of existing standards to respond to the need, and 4) the extent and stage of the deployment of affected technologies. "[11] Priority Action Plans (PAP)[12] were established to address technical updates and other outstanding issues for

[8] Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, Office of the National Coordinator for Smart Grid Interoperability, NIST Special Publication 1108, January 2010. http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf

[9] FERC, Smart Grid Policy Statement Docket No. PL09-4 (July 16, 2009) *available at* http://www.ferc.gov/whats-new/comm-meet/2009/071609/E-3.pdf. (*Policy Statement*)

[10] Ibid 6, p.5.

[11] Ibid [7] p.75

[12] Priority Action Plans (PAPs) are targeted task plans designed to resolve differences and develop recommendations related to a specific standards issue. PAPs are staffed and managed by volunteers from industry user groups and SDOs. http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PriorityActionPlans

each of these potential standards. Products from the PAPs will provide the initial candidates for *standards*.

Table 1. NIST Priority Action Plans[13]

#	Priority Action Plan	#	Priority Action Plan
0	Meter Upgradeability Standard	1	Role of IP in the Smart Grid
2	Wireless Communications for the Smart Grid	3	Common Price Communication Model
4	Common Schedule Communication Mechanism	5	Standard Meter Data Profiles
6	Common Semantic Model for Meter Data Tables	7	Electric Storage Interconnection Guidelines
8	CIM for Distribution Grid Management	9	Standard DR and DER Signals
10	Standard Energy Usage Information	11	Common Object Models for Electric Transportation
12	IEC 61850 Objects/DNP3 Mapping	13	Time Synchronization, IEC 61850 Objects/IEEE C37.118 Harmonization
14	Transmission and Distribution Power Systems Model Mapping	15	Harmonize Power Line Carrier Standards for Appliance Communications in the Home
16	Wind Plant Communications	17	Facility Smart Grid Information Standard

EISA directs FERC to "…institute rulemaking proceedings to adopt standards necessary to insure functionality and interoperability in interstate transmission of electric power, and regional and wholesale electricity markets."[14] More specifically, FERC's Smart Grid Policy Statement interprets EISA as granting FERC the authority to "…adopt smart grid standards—such as meter communications protocols or standards—that affect all facilities, including those that relate to distribution facilities and devices deployed at the distribution level, if the Commission finds that such standards are necessary for smart grid functionality and interoperability in interstate transmission of electric power, and in regional and wholesale electricity markets."[15]

"EISA, however, does not make any standards mandatory and does not give the Commission authority to make or enforce any such standards. Under current law, the Commission's authority, if any, to make smart grid standards mandatory must derive from the Federal Power Act. "[16]

[13] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WebHome#Priority_Action_Plans_PAPs
[14] EISA sec. 1301 and sec. 1305(d)
[15] Ibid [13] p15. NOT SURE WHAT THIS REFERENCE IS TO…
[16] Ibid [13] p15.

3. Where will smart grid standards come from?

Standards are developed and maintained by standards development organizations or standards bodies, also referred to as SDOs. Well-known standards organizations include the ISO, W3C, IEEE, NEMA, NAESB, and OASIS.

For smart grid, NIST is the organization designated under EISA to lead and manage standards development activities. Specifically, NIST has primary responsibility" to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems…"[17] To carry out this charge, NIST is collaborating with the GWAC, numerous expert working groups and SGIP Cyber Security Working Group to identify and recommend standards to address each of the various components of smart grid.

NIST formed the Smart Grid Interoperability Panel (SGIP) in order to establish a governing board of industry representatives to help guide the identification and development of *standards*. The SGIP is a public-private partnership structured to provide the broad industry representation necessary to review recommendations from each of the working groups and assure they reflect the consensus required to support standards adoption. Recommendations from the NIST working group and PAPs will be passed to different SDOs for development of the actual *standards*. EISA specifically names and refers to the following standards organizations that will play a role in smart standards development:

- Institute of Electrical and Electronics Engineers (IEEE)
- National Electrical Manufacturers Association (NEMA)
- International Electrotechnical Commission (IEC)
- American National Standards Institute (ANSI)
- German Standards Institute (Deutsches Institut für Normung)
- International Organization for Standardization
- International Telecommunication Union
- Society of Automotive Engineers (SAE) to address electric vehicles
- North American Electric Reliability Corporation (NERC).

Standards relevant to smart grid are also likely to involve many other organizations representing the utility, consumer electronics, and other related industries.

4. What is the process for developing standards related to Smart Grid?

NIST structured an open and collaborative process with a broad set of industry stakeholders to assure that no single voice has the ability to unfairly influence a standard. Each of the SDOs has its own review and adoption processes which involve additional and separate stakeholder representation. The NIST process was designed with several review and approval points and a strong system of checks and balances to assure that standards reflect industry needs. The NIST process can be broken down into three stages.

[17] EISA 2007, Section 1305(a) http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h6enr.txt.pdf

- Stage 1: Develop Requirements

  NIST created the SGIP with an elected Board of Governors representing 23 industry stakeholder categories to oversee and manage the requirements development process and other activities of the SGIP. One stakeholder category is reserved to represent state and local regulatory interests. Affected federal agencies are represented by a separate stakeholder category. Any individual or organization can approach SGIP or an SDO at any time to suggest an activity to develop requirements for a standard. Working groups associated with each PAP are open to industry participation. With NIST leadership, each PAP is charged with identifying requirements and issues. Products from the PAPs and other working groups are subject to a structured, open review process which when finalized are passed to an SDO for consideration and development or modification of a standard.

- Stage 2: Develop/Modify the Standard

  While the standard development process can vary substantially across SDOs, all include structured reviews by committees of industry representatives. In some cases, the SDO committees may include some or all of the same individuals involved in a PAP. The SDO uses the PAP requirements as a basis for drafting or updating a standard.

- Stage 3: FERC Review and Adoption

  NIST reviews and determines which SDO standards should be considered by FERC based on how the standard addresses the requirements identified by the SGIP and the NIST roadmap and passes a cyber-security review. FERC review and development of standards is a highly structured, codified process requiring public notice, hearings, testimony and published decisions.

There are at least five opportunities within the NIST process where an open forum is created for stakeholders, including state regulators and staff, to participate and provide input to the standards development and adoption process: the SGIP, PAPs, NIST working groups, SDOs, and through written comments and potential testimony during FERC public proceedings.

It is important to note that the actual language and structure of the standard will be guided by the PAP and finalized in the SDO process. To influence development of a standard would require regulators or staff to actively participate in either the PAP or SDO. Once a standard is developed and adopted by an SDO, any changes suggested by FERC or a state will require the SDO to reconsider changing the standard itself.

Standards can change over time due to evolutionary changes to technology, the law or other factors, which may in turn require state commissions and FERC to re-adopt a standard.

How FERC concludes its review could influence state commission options. States have the option to establish their own proceedings and to consider how a particular standard might be applied within their jurisdiction.

5. What smart grid standards is NIST developing?

Under EISA 2007 NIST is only charged with coordinating the development of *standards*. All *standards* will be prepared by SDOs and other industry groups.

Consistent with EISA, NIST coordinated activities with NEMA to introduce the first smart grid standard on September 24, 2009: SG-AMI 1-2009 Requirements for Smart Meter Upgradeability,[18] which defines firmware upgrade requirements for advanced meters and provides guidance to utilities, state commissions and other interested parties that deploy AMI. The NEMA standard provides a set of voluntary requirements that will provide AMI with flexibility and upgradeability to comply with emerging requirements for the smart grid.

NIST is currently coordinating the development of two sets of *standards*, both of which are identified and described in the "Roadmap" report.[19] The first set includes 25 *standards*[20] (see Table 3 at the end of this document) which NIST believes have strong stakeholder consensus based on feedback from multiple workshops, working group discussions, and public comments.[21] Many of these 25 *standards* have been in voluntary use within the power industry for years and have already been approved or are in the process of being approved by recognized SDOs.

NIST also identified a second set of 50 additional candidate *standards* and emerging specifications that are likely to have applicability to smart grid (Roadmap report, Table 4-2). This second set of candidate *standards* will require a more thorough review and consensus development process before they are ready for consideration. This expanded list was identified as a product of an EPRI-NIST sponsored workshop in May 2009.

Section 2. Smart Grid Standards Proposed by NIST for adoption by FERC

Consistent with EISA, NIST has identified the first five smart grid standards for consideration by FERC. Many additional *standards* covering a broad array of technical and policy issues are in various stages of development with release dates beginning in early 2011. As part of its technical support to the FERC/NARUC Collaborative on Smart Response, LBNL will review and highlight potential issues for state regulators for each of the proposed NIST *standards* once they have been finalized, released for public review, and forwarded to FERC.

FERC is required under EISA to institute rulemaking proceedings to adopt *standards* necessary to support smart grid. However, EISA does not provide FERC with authority to mandate or enforce standards. Therefore, the potential impacts of proposed smart grid standards will be dependent upon actions by other federal agencies, states commissions, individual utilities or other voluntary market participants that could choose to mandate otherwise voluntary FERC standards. As a result, LBNL review memos of proposed Smart Grid standards should be viewed as evolving assessments at a specified point in time, which may need to be periodically updated to reflect FERC, state, and other agency decisions.

1. What smart grid standards is NIST submitting to FERC?

On Oct. 6, 2010, NIST identified five smart grid standards for consideration by FERC.[22] At least four of these five *standards* were previously approved by the IEC and have been in broad use for several years by utilities and vendors. Table 2 lists the five proposed *standards*, their key attributes,

---

[18] http://www.nema.org/stds/sg-ami1.cfm
[19] Ibid [7]
[20] This first set of 25 standards is an expansion of the original list of 17 standards.
[21] In April 2009, NIST identified 16 existing standards and other specifications that could be applied immediately or were expected to be available within a reasonable time frame. This list was published in the Federal Register for review and comment. NIST eventually added nine additional standards, all of which were subject to public review.
[22] http://www.nist.gov/public_affairs/releases/upload/FERC-letter-10-6-2010.pdf

provides a link to the full standard language, and a cross reference to their listing in the NIST Roadmap report (see Table 3).

Table 2. First Five Smart Grid Standards Referred From NIST to FERC

NIST Roadmap Ref #	Standard [link]	Description
5	IEC 60870-6 Inter-Control Center Protocol Standard IEC_60870_Narrative_10-6-2010.doc	Specifies the method of exchanging ISO-compliant time-critical data between utility control centers ▪ Includes the exchange of real-time data indications, control operations, time-series data, scheduling and accounting information, remote program control, and event notification. ▪ Used between control centers in almost every utility for communication. ▪ Benefits are measured in terms of reliability and interoperability. Example: Transmission line failure reported to multiple utilities in multiple jurisdictions in real time. Important to state regulators because: ▪ This standard defines the way utilities are linked together today ▪ It facilitates the wide area system control which is critical to safe and reliable operation
6	IEC 61850 Substation Automation Standard IEC_61850_Narrative_10-6-2010.doc	Provides a standardized framework for substation automation and integration ▪ Specifies the communications requirements, functional characteristics, structure of data in devices, the naming conventions for the data, how applications interact and control the devices, and how conformity to the standard should be tested. ▪ Key attributes are ease of multi-vendor integration, low installation costs, faster and more accurate system configuration ▪ Results in fewer errors, more capability and flexibility than previous standards ▪ Implements modern networking technology in the substation Example: Facilitates unambiguous exchange of information between multiple vendor systems Important to state regulators because: ▪ Substations are the core of a distribution system ▪ Key to eliminating vendor lock-in in substations ▪ In use since 2002, used worldwide, uses modern networking and computer technology, field proven, and shown to be highly reliable
7	IEC 61968 Common Information Model Standard (Distribution) IEC_61968_Narrative_10-6-2010.doc	Allows data to move seamlessly to and from different metering systems and among other system software and components such as: ▪ Meter data collection software, the control center/back office, translation software, billing systems, and other enterprise business software systems. ▪ Software data exchange used in asset tracking and work force management Example: Allows data to move from multiple vendor meters and head ends through multiple software systems into the billing system. Important to state regulators because: ▪ Describes the interface between the metering system and distribution management systems which is the link between AMI and the Smart Grid

NIST Roadmap Ref #	Standard [link]	Description
		▪ Simpler and less expensive than multiple proprietary formats which are more complicated and expensive to use than a single CIM. ▪ Benefits result from economy of scale, less complexity, and interoperability and will decrease problems with data transfer in multi-state utilities.
7	IEC 61970 Common Information Model (CIM) Standard IEC_61970_Narrative_10-6-2010.doc	Foundational - provides basic methods of describing power system components in a structured manner readily interpreted by software systems (similar to how HTML is the foundation for web applications) ▪ Describes the components of a power system and the relationships between each component. ▪ Facilitates the exchange of data between multiple utilities ▪ Within a company, allows the exchange of data between applications, such as work scheduling, asset tracking, etc. <u>Example</u>: Planning group sends characteristics of new transmission line to operations – CIM describes what the line will look like physically and electrically. <u>Important to state regulators because:</u> ▪ The CIM facilitates unambiguous exchange of information between utility and RTO/ISO software systems ▪ It saves utilities system integration expense when extending/upgrading energy management and control center systems ▪ Minimizes likelihood of vendor lock-in in utility back office enterprise software systems
22	IEC 62351: Cyber Security Standard IEC_62351_Narrative_10-6-2010.doc	Applies to each of the other standards. ▪ Adds more reliability to the system by mitigating cyber attacks ▪ Replaces the "security by obscurity" concept used in the past Example: Secures link between utility and substation - minimizes chances that hacker can issue control commands to substation and feeder equipment. Security objectives include ▪ Authentication of entities through digital signatures ▪ Ensuring only authorized access ▪ Prevention of eavesdropping, playback and spoofing ▪ Provides some degree of intrusion detection. <u>Important to state regulators because</u> ▪ It affects information security of power systems' standards ▪ Critical to the prevention of cyber attack induced system failures from nuisances to catastrophic ▪ Most likely of the five to need to be mandated in specific situations

2. Why should state regulators care about these *standards*?

While the technical aspects of these *standards* may not be at issue, state regulatory commissions should be aware of three potential impacts.

1) Not all utilities within a particular state jurisdiction may employ systems and operational practices consistent with the proposed *standards*. Extending these *standards* to all utilities within a jurisdiction may require additional investments which will have cost and related rate impacts.
2) All of the proposed *standards* address distribution system issues, which are traditionally under state jurisdiction. While FERC does not have the authority under EISA to mandate or enforce smart grid standards, adoption by FERC, NERC, or other federal organizations could create jurisdictional issues where federal standards impose system cost, operational requirements, and rate impacts on retail customers.
3) Adoption of these *standards* at either a state or federal level will alter the voluntary approach that currently exists, where each utility now independently determine whether or not to adopt a certain standard. Adoption at a state level would mandate the technical implications and requirements of these *standards* on all utilities subject to the jurisdiction of a state regulatory commission. Mandating *standards* within one state could impact interconnection agreements on utilities with multi-state operations.

3. Can state regulators rely on these *standards*?

Each of the five proposed NIST *standards* have been vetted and adopted by a recognized SDO and have been voluntarily implemented and in use by most utilities and major vendors for many years. There is widespread industry support for each of these *standards*. As a result, none of these five *standards* should pose any major issues or create unintended consequences.

4. What are the cost implications of these *standards*?

The first five *standards* proposed by NIST should have few if any cost implications for utilities or state commissions.

Direct costs may be incurred by individual utilities who have not implemented these *standards* if state regulatory commissions mandate implementation. If a state regulatory commission issues a decision that adopts these five standards, utilities under their jurisdiction may incur indirect costs if lack of adherence or implementation results in restricted or adverse impacts due to the inability to support control center communications, distribution automation applications, or lack of adherence to cyber security requirements.

5. Would adoption of these five *standards* constrain regulatory choices?

The first five *standards* proposed by NIST should have minimal infrastructure implications, consistent with the responses to questions 2 and 4.

6. What impact would adoption of these *standards* have on privacy?

Each of the first five standards proposed by NIST should have little if any impact on privacy. These five *standards* address control center, transmission and distribution, and back office systems that should not directly interact with or impact individual customer information.

Privacy issues are generally focused on "personally identifiable" information that is directly related or linked to individual customers. Recent publications, such as the NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (SP 800-122)[23] and Office and Management and Budget memorandums address privacy as follow:

> "Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as a date and place of birth, mother's maiden name, etc."[24]

7. What is the cyber security review of these *standards*?

The first five *standards* proposed by NIST were adopted by the IEC to address control and communication for the grid. Each of these *standards* has been evaluated under the SGIP-NIST process as well as the NERC Critical Infrastructure Protection program. IEC-62351, the last of the five proposed *standards*, includes eight sections that focus specifically on cyber security requirements for distribution automation and control system elements in the other four *standards*.

8. How can regulators and staff participate in the development or adoption of *standards*?

There are two schools of thought on this question. The first perspective is that regulation is focused on the 'what,' not the 'how.' These *standards* typically address very detailed technical issues predominantly focused on the 'how,' where little interaction should be required from state commissions. Each state could simply accept the output of the SDO process, and provide guidance to their stakeholders regarding their view of the standard and how it could or should be implemented in their jurisdiction. Regulators have the opportunity to either direct or encourage utilities subject to their jurisdiction to participate in the development of *standards* and provide technical input that reflects their perspective on issues under discussion and/or reflects state policies.

A second perspective is that states ought to take a proactive stance and participate in the SGIP or SDO process on specific *standards*. State commissions that want a more active role in the *standards* development process can participate in a variety of forums, each with varying levels of commitment. Examples include:

1) Participate as individual state commissions or through NARUC committees to identify problem areas and make recommendations for consideration in the NIST SGIP forum. Industry working groups aligned with various professional organizations outside the NIST process also provide opportunities to work with SDOs and propose or develop standards.
2) Participate in any of the 17 PAPs or related working groups that are establishing the requirements that will eventually form the basis for SGIP adoption and assignment to an SDO, either as an observer or more active partner.
3) Join technical committees within individual SDOs.
4) Write comments or testimony for FERC proceedings.

The first two options provide greater opportunities to influence and structure the actual requirements that lead to a potential standard. However participation at this level can require

[23] http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf
[24] http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

extensive time commitment. Once a potential standard moves to an SDO, options to modify the specific requirements are substantially reduced. Time commitments during the SDO process may be even greater than within the PAP. Participation in FERC proceedings is generally limited to commenting on elements of a standard. The FERC process affords much less opportunity to influence the substance of a particular standard and comes with much higher risks that adoption will lead to cost and jurisdictional impacts. For example, while EISA does not provide FERC with enforcement power, several of the NIST coordinated smart grid standards could be interpreted to have application under FERC bulk-power system authorities.[25]

9. How can regulators stay current with everything that is happening?

In a perfect world, there would be enough staff, time, and budget for every state regulatory commission to participate in the review and development of every standard to insure their issues and concerns are addressed early in the process. The approach established by NIST to meet the requirements of EISA address an extraordinary range of complex issues that have been compressed into a very short standards development process. Staying abreast of the PAPs, working groups and other development activities is difficult.

Commissions can participate directly in the email blogs for the SGIP and each of the PAP and working groups, which will provide almost continuous updates on meetings, products, and the status of related activities. Detailed information on each of the PAP meeting schedules, development status, products, and contacts can be found through by following the links in Table 1.

In an effort to help simplify this incredible volume of information, NARUC, FERC, LBNL, NIST/SGIP and EnerNex (the contractor tasked with supporting the SGIP) are collaborating to provide periodic webinars and briefing documents for state regulators and staff to keep them current on the development process and help focus state commission discussions and involvement.

[25] Federal Energy Regulatory Commission, Policy Statement, p.11, http://www.ferc.gov/whats-new/comm-meet/2009/071609/E-3.pdf

Table 3. NIST Roadmap Report - Top 25 Proposed Critical Smart Grid Standards[26]

	Standard [Link]	**Description**
1	ANSI/ASHRAE 135-2008/ISO 16484-5 BACnet http://resourcecenter.ashrae.org/store/ashrae/newstore.cgi?itemid=30853&view=item&page=1&loginid=39839941&priority=none&words=135-2008&method=and&	BACnet defines an information model and messages for building system communications at a customer's site.
2a	ANSI C12.1 http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+C12.1-2008	Performance and safety type tests for revenue meters.
2b	ANSI C12.18/IEEE P1701/MC1218 http://webstore.ansi.org/FindStandards.aspx?SearchString=c12.18&SearchOption=0&PageNum=0&SearchTermsArray=null|c12.18|null	Protocol and optical interface for measurement devices.
2c	ANSI C12.19/MC1219 http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+C12.19-2008	Revenue metering End Device Tables.
2c	ANSI C12.20 http://webstore.ansi.org/FindStandards.aspx?SearchString=c12.20&SearchOption=0&PageNum=0&SearchTermsArray=null|c12.20|null	Revenue metering accuracy specification and type tests.
2e	ANSI C12.21/IEEE P1702/MC1221 http://webstore.ansi.org/FindStandards.aspx?SearchString=c12.21&SearchOption=0&PageNum=0&SearchTermsArray=null|c12.21|null	Transport of measurement device data over telephone networks.
3a	ANSI/CEA 709.1-B-2002 http://www.ce.org/Standards/browseByCommittee_2543.asp	Control Network Protocol Specification. This is a general purpose local area networking protocol in use for various applications including electric meters, street lighting, home automation and building automation. This is a specific physical layer protocol
3b	ANSI/CEA 709.2-A R-2006 http://www.ce.org/Standards/browseByCommittee_2545.asp	Power Line (PL) Channel Specification. This is a specific physical layer protocol designed
3c	ANSI/CEA 709.3 R-2004 http://www.ce.org/Standards/browseByCommittee_2544.asp	Twisted-Pair Channel Specification. This protocol provides a way to tunnel local operating network messages through an IP network
3d	ANSI/CEA-709.4:1999 http//www.ce.org/Standards/browseByCommittee_2759.asp	Fiber-Optic Channel Specification
4	DNP3 http://www.dnp.org/About/Default.aspx	Use for substation and feeder device automation as well as for communications between control

[26] Ibid [5]

	Standard [Link]	**Description**
		centers and substations.
5	IEC 60870-6 / TASE.2 http://webstore.iec.ch/webstore/webstore.nsf/artnum/034806	Defines communications within transmission and distribution. substations for automation and protection.
6	IEC 61850 Suite http://webstore.iec.ch/webstore/webstore.nsf/artnum/033549!opendocument	Defines communications within transmission and distribution. substations
7	IEC 61968/61970 Suites http://webstore.iec.ch/webstore/webstore.nsf/artnum/031109!opendocument http://webstore.iec.ch/webstore/webstore.nsf/artnum/035316!opendocument	Define information exchanged among control center systems using common information models.
8	IEEE C37.118 https://sbwsweb.ieee.org/ecustomercme_enu/start.swe?SWECmd=GotoView&SWEView=Catalog+View+(eSales)_Standards_IEEE&mem_type=Customer&SWEHo=sbwsweb.ieee.org&SWETS=1192713657	Defines phasor measurement unit (PMU) performance specifications and communications.
9	IEEE 1547 Suite https://sbwsweb.ieee.org/ecustomercme_enu/start.swe?SWECmd=GotoView&SWEView=Catalog+View+(eSales)_Standards_IEEE&mem_type=Customer&SWEHo=sbwsweb.ieee.org&SWETS=1192713657	Defines physical and electrical interconnections between utility and distributed generation (DG) and storage.
10	IEEE 1588 http://ieee1588.nist.gov/	Standard for time management and clock synchronization across the Smart Grid for equipment needing consistent time management.
11	Internet Protocol Suite including IETF RFC 2460 (IPv6) http://www.ietf.org/rfc/rfc2460.txt	Foundation protocol for delivery of packets in the Internet network
12	Multispeak http://www.multispeak.org/About/specifications.htm	Specification for application software integration within the utility operations
13	OpenADR http://openadr.lbl.gov/pdf/cec-500-2009-063.pdf	Specification defines messages between utilities and commercial/industrial customers for price-responsive and direct load control.
14	OPC-UA Industrial http://www.opcfoundation.org/Downloads.aspx?CM=1&CN=KEY&CI=283	Exchange of location-based information addressing geographic data requirements
15	Open Geospatial Consortium Geography Markup Language (GML) http://www.opengeospatial.org/standards/gml	Exchange of location-based information addressing geographic data requirements for many Smart Grid applications.
16	ZigBee/HomePlug Smart Energy Profile 2.0 http://www.zigbee.org/Products/TechnicalDocumentsDownload/tabid/237/Default.aspx	Home Area Network (HAN) Device Communications and Information Model.
17	OpenHAN http://osgug.ucaiug.org/utilityami/openhan/HAN%20Requirements/Forms/AllItems.aspx	Specification for home area network (HAN) to connect to the utility advanced metering system
18	AEIC Guidelines v2.0	Framework and testing criteria for vendors and

	Standard [Link]	**Description**
		utilities who desire to implement standards-based Advanced Metering Infrastructure (AMI).
19	Security Profile for Advanced Metering Infrastructure, v 1.0, Advanced Security Acceleration Project – Smart Grid, December 10, 2009 http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/AMI%20Security%20Profile%20(ASAP-SG)/AMI%20Security%20Profile%20-%20v1_0.pdf.	Guidance and security controls to organizations developing or implementing AMI solutions. This includes the meter data management system (MDMS) up to and including the HAN interface of the smart meter.
20	Department of Homeland Security, National Cyber Security Division. Catalog of Control Systems Security: Recommendations for Standards Developers. http://www.us-cert.gov/control_systems/pdf/FINAL-Catalog_of_Recommendations_Rev4_101309.pdf	Compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyber attacks.
21	DHS Cyber Security Procurement Language for Control Systems http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_100809.pdf	Guidance to procuring cyber security technologies for control systems products and services - it is not intended as policy or standard
22	IEC 62351 Parts 1-8 http://webstore.iec.ch/webstore/webstore.nsf/artnum/037996!opendocument	Defines information security for power system control operations.
23	IEEE 1686-2007 https://sbwsweb.ieee.org/ecustomercme_enu/start.swe?SWECmd=GotoView&SWEView=Catalog+View+(eSales)_Standards_IEEE&mem_type=Customer&SWEHo=sbwsweb.ieee.org&SWETS=1192713657	Defines the functions and features to be provided in substation intelligent electronic devices (IEDs) to accommodate critical infrastructure protection programs.
24	NERC CIP 002-009 http://www.nerc.com/page.php?cid=2|20	Covers physical and cyber security standards for the bulk power system.
25	NIST Special Publication (SP) 800-53, NIST SP 800-82 http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf; http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf.	Covers cyber security standards and guidelines for federal information systems, including those for the bulk power system.