UNITED STATES OF AMERICA

BEFORE THE

DEPARTMENT OF ENERGY

Implementing the National Broadband Plan by	)
Empowering Consumers and the Smart Grid:	)
Data Access, Third Party Use, and Privacy	)

TO: The Office of the General Counsel

COMMENTS OF THE
AMERICAN PUBLIC POWER ASSOCIATION

In response to the U.S. Department of Energy's ("DOE") Request for Information ("RFI") published May 11, 2010 in the *Federal Register*,[1] the American Public Power Association ("APPA") hereby submits its comments in response to questions on data access, third party use, and privacy as related to the implementation of smart grid technology.

APPA is the national service organization representing the interests of not-for-profit, publicly owned electric utilities throughout the United States. More than 2,000 public power systems provide over 15 percent of all kilowatt-hour sales to ultimate customers and do business in every state except Hawaii. APPA utility members are load-serving entities, with the primary goal of providing customers in the communities they serve with reliable electric power and energy at the lowest reasonable cost, consistent with good environmental stewardship. This orientation aligns the interests of APPA-member electric utilities with the long-term interests of the residents and businesses in their communities. Collectively, public power systems serve 45 million people.

---

[1] 75 Fed. Reg. 26,203 (May 11, 2010).

APPA recognizes that successful utility implementation of Smart Grid technologies hinges, in part, on creating and maintaining customer confidence that utilities and third party service providers have appropriate security protocols in place to address data access and customer privacy concerns. APPA believes that public power utilities can best address most data access and privacy issues related to smart grid implementation through their currently-applicable legal, regulatory, and managerial frameworks. These frameworks provide proven processes for addressing these issues (many of which are not new). Use of these processes will also help in identifying instances where additional laws, regulations, or utility policy revisions are needed.

Privacy and data access policies should be determined at the state and local level for the most part. For example, public power utilities typically rely on state law and legal precedents, local ordinances, and guidance from their governing bodies to set policy.

National involvement, however, could be useful in certain areas. For example, DOE's current RFI process should be extremely helpful in identifying areas of agreement and disagreement regarding privacy and data access issues. Also, DOE could provide continued support by compiling examples of policy guidelines and sample privacy policies. (It might be useful to coordinate this activity with the National Association for Regulatory Utility Commissioners ("NARUC"), as its member commissions are likely to be the entities reviewing and adopting such policies for investor-owned utilities.) Another area for national involvement concerns ensuring the cyber security of the data collected via smart meters, as customers want to know that their personal information will be safe from hackers or interception by outside parties. DOE's companion RFI on communications requirements for smart grid[2] specifically addresses security issues, so APPA's privacy comments will note only one important national initiative relating to cyber security and the smart grid. The National Institute of Standards and

[2] 75 Fed. Reg. 26,206 (May 11, 2010).

Technology's ("NIST") smart grid standards project is an ongoing initiative, involving numerous stakeholders, to set cyber security guidelines that are technology neutral and provide for interoperability. The development of these standard security protocols will help utilities as they make decisions on smart grid investments and communication technology.

For a public power utility, the decision whether, when, and how to implement smart grid technology will depend on many utility-specific factors, including the utility's load profile, the age and operational efficiency of existing equipment, the financial health of the system, community receptivity and input, and the cost of different options compared to the prospective benefits. The utility must comply with existing state and local laws concerning data access, and the local regulatory body – typically either the city council or independent utility board – must approve the utility's capital investment, strategic plans, and any revisions to associated utility policies.

APPA expects that there will be considerable diversity in how public power utilities move forward with the implementation of smart grid technologies. Some utilities will elect to make incremental investments in smart grid technology, with the first steps aimed at improving digital communication within the distribution system. Smart meter implementation may come later and may focus initially on industrial and commercial customers. Other utilities will adopt more ambitious smart grid plans providing for a single roll out of smart meters for all customers while also pursuing improved distribution system efficiencies.

Even when a utility extends its smart meter program to residential customers, the initial goals may be increased operational efficiency, improved reliability, and the provision of basic usage information to customers. For another utility, important initial goals may be implementation of real-time pricing and the provision of real-time consumption data. These

implementation decisions and goals, proposed by the utility's management and approved by the utility's regulatory body with appropriate input from the community, will affect how the utility provides consumption data to its customers.

DOE's RFI seeks comments on specific questions, and APPA addresses each of these eighteen questions, below.

1) Who owns energy consumption data?

Utilities implement smart grid technologies in order to improve operating efficiency and system reliability and to provide customers with better information to promote informed decision-making about electricity use. These improvements can include better outage management and service restoration, enhanced voltage control, identification of possible preventive maintenance, and implementation of innovative rate plans and demand response initiatives. Utility investment in smart meters would be pointless unless the utility had the ability to use the data collected by the meters for these purposes. The utility (especially smaller public power systems) may also need to engage third party contractors to manage the extensive data generated by smart meters. In addition, some utilities already use third-party contractors to handle billing functions, or to assist in other utility functions, such as service restoration after outages occur. Third party contractors that a public power system engages to assist with these functions must have unrestricted access to the data for the purposes of providing such utility-related services. APPA sees these services as part and parcel of the public power system's provision of "core" utility service, and does not believe that individual customer permission should be required for public power systems to engage in these activities. APPA does believe that third party contractors obtaining potentially sensitive customer data should undertake to protect it from unauthorized disclosure.

Customers should be able to control whether – and how – they want to share their own consumption data with independent third party providers, for example, providers of energy management services, in-home devices and home area network ("HAN") applications.

Thus, APPA supports a model under which utilities and their customers "co-own" smart meter data as it is used in utility business functions, and customers "own" their consumption data for the purpose of participating in independent third party providers' products and services.

2) Who should be entitled to privacy protections relating to energy information?

Utility customers have an expectation of privacy related to information maintained by the utility, and honoring that expectation will be an important component of customer acceptance of smart grid technologies. In general, state law has the strongest role in setting basic privacy protections for customers of public power utilities, because these utilities are units of government and are often subject to information disclosure statutes applicable to governmental entities. Public power utilities will interpret state statutes as they relate to the additional information provided by smart meters. Some jurisdictions may elect to revise public disclosure statutes to specifically address smart meter data. (For example, when Texas enacted its electricity restructuring law in 1999, the state also revised public disclosure laws to allow public power utilities to keep confidential information that was deemed competitive.) As smart grid installations become more prevalent, some jurisdictions may adopt specific laws regarding the release of customer information to third parties to address issues surrounding customer consent and privacy,

3) What, if any, privacy practices should be implemented in protecting energy information?

Effective privacy practices are predicated on customer choice, meaningful notice, and transparency. In general, both utilities and third party providers should consider these guidelines in establishing privacy practices: (i) limit the collection of information to that which is reasonably necessary to support the utility's business operations; (ii) provide clear disclosures to customers about the type of information collected and the uses to which the information will be put; (iii) establish privacy rules that are visible and transparent for customers; (iv) require prior customer consent to release customer information to independent third party providers and only to the extent authorized by the customer; (v) implement technology and practices that ensure the integrity of the collected data through the entire life cycle of customer information; (vi) provide customers with access to their data maintained by the utility in a manner that is convenient and transparent; (vii) establish procedures for timely notification in the event of breach or inadvertent disclosure of customer information; and (viii) implement security safeguards to protected against unauthorized access, disclosure and destruction. Public power utilities also must ensure that their privacy and data policies are consistent with state and local laws and regulations.

When possible, utilities should use secure communication technologies to transfer smart meter data. This would include utility-owned fiber optic lines, broadband over power lines, or other wired communication technologies. Where this is not practical or possible and utilities must use wireless or commercial communication paths, or when data are transferred over the Internet, utilities should follow industry standards for encryption of sensitive energy information.

4) Should consumers be able to opt in/opt out of smart meter deployment or have control over what information is shared with utilities or third parties?

Smart meters are part of a utility's infrastructure and its operating structure. Some utilities may choose to implement smart meters and other control programs with larger customers only, and these programs could be voluntary, with customers deciding whether they want to participate. (Often, these programs are implemented to achieve demand reductions, rather than to improve system operations.)

However, once a utility decides on a system-wide deployment of smart meters (or a class-wide deployment, *e.g*., all industrial or large commercial customers), it would be administratively burdensome for the utility to allow individual customers to opt out. A public power utility that deploys smart meters to all customers in a class is making the investment in order to achieve substantial operational and reliability benefits. The deployment includes many other investments in addition to the meters, for example contracting for data management systems and upgrading the utility's billing system to handle the large amount of data produced by the smart meters. If customers could opt out, the utility would not get the maximum benefit from its data management and billing systems, and the utility would have to continue to employ personnel to read and maintain the alternate meters.

As described in response to question #1, utilities must be able to use data collected from smart meters for utility-related business purposes such as operating and maintaining the system, managing outages, managing load, and automating billing procedures. Once a utility deploys smart meters, customers would still have options, including control over whether they want to share their own data with third party energy service marketers and deciding whether or not to participate in voluntary utility rate and demand response programs.

5) **What mechanisms should be made available to consumers to report concerns or problems with the smart meters?**

Public power utilities have existing processes in place to address customer complaints about billing, customer service, and power quality. Those same processes can readily accommodate customer inquiries and concerns about smart meters. Typically, a public power utility's customer service department responds to complaints regarding meters. If issues persist, customers can raise any issues with higher levels of management or the utility's governing body (city council or independent utility board). Public power utilities pride themselves on good customer relationships. Utility managers, council members, and board members all are members of the community, and this local control makes public power utilities responsive to customer needs.

6) **How do policies and practices address the needs of different communities, especially low-income rate payers or consumers with low literacy or limited access to broadband technologies?**

Low-income residential customers often have significantly lower than average electricity consumption and therefore have fewer opportunities to cut back on electricity use. They are less likely to benefit from real-time pricing programs and, in fact, may see higher bills. Hence, time-of-use rates should be introduced carefully to this customer class. For example, an increasing block rate tariff that sets the first block at a reasonable volume for low-income customers could encourage conservation without unduly penalizing these customers. Some utilities have implemented prepaid billing plans. Salt River Project, a public power utility in Phoenix, Arizona, offers a plan that includes in-home display units showing the amount of credit left on the prepay

card and how many days the credit should last based on the customer's usage. Participants in the plan report that the plan helps them control their bills.[3]

Utilities will have different plans for how to use smart meter data. Some will focus first on improving operational efficiency and reliability, rather than immediately implementing real-time pricing programs or providing real-time consumption data. Instead, these utilities could offer residential customers a time-of-use ("TOU") pricing option based on system averages and provide daily or weekly consumption data on a delayed basis. This type of pricing and information program can reduce the utility's peak demand but be more cost-effective than providing detailed and real-time energy data. Customers that want more control over their energy use – and have the most to gain from reducing energy consumption – would be able to purchase energy management software, either from the utility, or from a third party provider. At the same time, low-income customers would not have to pay for system-wide installation of home energy management systems or sophisticated control devices.

In conjunction with implementing any TOU or real-time pricing programs, utilities will need to educate customers on the benefits of shifting electricity use away from peak times. Visual material, such as magnet charts showing on-peak and off-peak hours (for time-of-use pricing) or energy orbs/read-out devices that show high peak hours (for real-time pricing) or dollars remaining on a pre-paid plan could be effective ways of reaching low literacy customers or those with limited access to broadband.

Low-income or low-literacy customers do not need separate privacy policies, but may need more focused efforts, such as public meetings, to explain the utility's policies.

[3] See the Salt River Project plan, at http://www.srpnet.com/payment/mpower/default.aspx for plan details. Customer comments are found here: http://www.mysrpmpower.com/Share.aspx.

7) Which, if any, international, Federal, or State data-privacy standards are most relevant to Smart-Grid development, deployment, and implementation?

Relevant standards include state information and public disclosure laws, regulations issued by public utility commissions (Texas and California are two states currently addressing customer privacy issues as related to smart grid technology), and the NIST process to develop cyber security guidelines. NIST included a preliminary set of privacy principles in its February 2010 draft report on smart grid cyber security.[4] Examples of the NIST principles include providing adequate notification on what information is collected and how it is to be used; limiting data collection to what is required for the utility's operations, including planning, management, improving energy use and efficiency, and account management; and providing a process to allow customers access to their energy information. Utilities and third-party energy service providers can consider these general principles in designing customer education material and developing or revising their own privacy policies. (As previously note, public power utilities must also make sure that their privacy and data access policies comply with state and local public disclosure laws.)

In addition, the Fair Credit Reporting Act, as amended by the Fair and Accurate Credit Transaction Act of 2003 ("FACTA"), provides some protection of customer information. Utilities must comply with FACTA's Red Flags Rule for preventing identity theft.[5]

---

[4] National Institute of Standards and Technology, "Smart Grid Cyber Security Strategy and Requirements," Draft NISTIR 7628, February 2010, Chapter 4.

[5] For more information, see http://www.ftc.gov/redflagsrule

8) **Which of the potentially relevant data privacy standards are best suited to provide a framework that will provide opportunities to experiment, rewards for successful innovators, and flexible protections that can accommodate widely varying reasonable consumer expectations?**

There is likely to be significant variation in public power systems' privacy policies depending on how their state and local jurisdictions view privacy questions. These are questions of balance, and there is room for variation and consideration of local values. Because of the applicability of state "government in the sunshine" laws, however, public power systems may have less room to "experiment" with data privacy standards than other, privately-owned entities.

9) **Because access and privacy are complementary goods, consumers are likely to have widely varying preferences about how closely they want to control and monitor third-party access to their energy information: what mechanisms exist that would empower consumers to make a range of reasonable choices when balancing the potential benefits and detriments of both privacy and access?**

Many utilities already employ Internet-accessible customer portals allowing access to utility bills, online bill payment, and information about utility services and programs, and these utility customer portals typically employ sophisticated security protocols. As utilities deploy smart grid technologies, utilities may find that providing customers access to smart grid information through existing customer portals is the most cost-effective option. Existing Internet technologies can be leveraged to provide customers access to their information and choice in determining whether or not to release consumption data to third parties.

Other options include basic in-home energy displays and more sophisticated displays or home area network ("HAN") energy management systems. Security and privacy protocols should be incorporated into each of the access options to ensure the integrity of the information, customer choice, and transparency.

10) What security architecture provisions should be built into Smart Grid technologies to protect consumer privacy?

The standards being developed through the NIST smart grid project will provide the best framework for determining security architecture for smart grid technologies. These technologies should be developed using open standards that allow for interoperability and innovation as smart grid technologies mature. Security and privacy protections should be considered and incorporated at the inception of technology development and not as a "bolt on" later in the process. Core requirements should provide for resiliency against cyber attacks through controls that detect and prevent the corruption or unauthorized access to data. Utilities should regularly access technology solutions for vulnerabilities and have well defined procedures to address cyber threats.

11) How can DOE best implement its mission and duties in the Smart Grid while respecting the jurisdiction and expertise of other Federal entities, states and localities?

DOE can continue to provide forums to collect information and debate issues. DOE's report on this RFI process should be helpful in identifying problem areas. DOE can also provide support by compiling information on case studies, policy guidelines, and sample privacy policies, and making this information easily available to the public. As noted above, it might be useful to involve NARUC in such efforts. FERC recently released the National Action Plan on Demand Response ("NAP-DR"), which includes many proposals for consumer education on demand response and smart grid. DOE and FERC now must submit to Congress an implementation plan for the NAP-DR. As part of the implementation plan, DOE could take an active role in some of the proposed projects, for example, developing a web clearinghouse for studies, reports, best practices, and other information.

Smart grid deployment is primarily a distribution utility issue, and so most deployment decisions should be made on the state or local level.

12) When, and through what mechanisms, should authorized agents of Federal, State, or local governments gain access to energy consumption data?

Currently, public power utilities must comply with relevant local, state and federal laws concerning the release of energy consumption data to governmental authorities. The additional data collected by smart grid would be covered under the same legal requirements. (For example, the applicable statute in the state of Washington provides that law enforcement agencies cannot request customer records from a public power utility unless the agency states in writing that it suspects that a crime has been committed and that it has a reasonable belief that the customer records will help determine if the suspicion is true.[6])

13) What third parties, if any, should have access to energy information? How should interested third-parties be able to gain access to energy consumption data, and what standards, guidelines, or practices might best assist third parties in handling and protecting this data?

In order to handle the massive amounts of information produced via smart grid technology and to use that information in connection with the provision of utility service, public power systems may contract with third parties to provide software, data collection, and data management services. The contract between public power systems and these third parties should include appropriate privacy and security provisions to protect customer data. These third parties are essentially an extension of the utility in conducting core utility services and therefore need to have access to the data comparable to that of the utility. This third-party access, however, should extend only to the performance of the contracted services, and utilities should impose security

[6] Washington Public Records Act, Revised Code of Washington 42.56.335.

and privacy requirements on the third party contractors to ensure the integrity of the information, protection of privacy, limited use of information, and appropriate destruction of stored data.

Independent third parties, such as those that market energy management services directly to customers, should only have access to energy consumption data if a customer has given permission. State and local regulatory bodies may consider adopting regulations covering how these third party marketers and service providers would communicate with customers on data access and privacy issues. For example, the process of obtaining a customer's permission should be transparent and require meaningful consent, that is, the process should ensure that the customer is aware that by signing up for the service, he or she is giving the third party access to the customer's energy usage information.[7] The third party should also include as part of its sign-up or sales process its own policy on sharing customer data with other parties and an explanation of how it will use the data collected. These explanations should be in easy to understand terms and prominently displayed.

14) What forms of energy information should consumers or third parties have access to?

Currently, most public power utilities provide monthly energy information to their customers. Many utilities are investing in smart grid technology, but they will not be able to provide detailed consumption information until they deploy smart meters. Many public power systems have made substantial investments in distribution automation, Supervisory Control and Data Acquisition ("SCADA") systems, automated meter reading and control devices. It may be the smartest course for a public power system to maximize the benefits of its current technology investments, by adding improved communications protocols, for example, and wait to invest in a

[7] DOE is no doubt aware of analogous problems in other industries, *e.g.*, long distance service, with overzealous third party providers of such services signing up customers for services they did not request; this practice was so prevalent that it acquired the nick-name "slamming."

large-scale meter deployment until NIST standards are issued, cyber security requirements are resolved, and there is more industry experience with smart grid technology.

Public power utilities have used load management and TOU rate structures to good effect for a long time. A utility that uses energy efficiency, demand response, and TOU programs to adequately control its load and achieve a significant portion of the estimated benefits of real-time pricing may not find it cost-effective to deploy smart meters at this time. Instead, such a utility would likely focus on implementing smart grid investments that improve its SCADA systems, distribution automation, and communications backbone.

A public power system that is investing in smart meter technology still will look to its business plan in determining what information to provide its customers. Some utilities will focus on efficiency and reliability issues and provide basic information to their customers in the first phase of implementation; other may choose to provide real-time information right away. Customers will typically have the ability (depending on the technology) to choose additional energy management services from third parties.

15) What types of personal energy information should consumers have access to in real-time, or near real-time?

A utility that has deployed smart meters will make this decision based on its smart grid technology and business plan. For some utilities, it will make sense to start providing detailed near real-time consumption data to customers upon installation, to help support time-differentiated or real-time rates and demand response programs. For other systems, providing real-time information may not initially produce enough benefits to warrant the cost. For example, such a utility may determine that providing residential customers access to usage data on a daily or weekly basis is sufficient to achieve the utility's peak-shaving goals. Under this option,

customers that want real-time data could take advantage of third party offerings of energy management tools.

The smart grid can give customers greater control over energy use and provide opportunities to change customer behavior to use energy more efficiently. The level of interest among customers will vary, and utilities will likely consider tailoring information access to different levels of customer engagement.

16) **What steps have the states taken to implement Smart Grid privacy, data collection, and third party use of information policies?**

State legislatures and public utility commissions have begun to address these issues in legislation, individual utility cases or in rulemakings. California and Texas are two examples.

17) **What steps have investor owned utilities, municipalities, public power entities, and electric cooperatives taken to implement Smart Grid privacy, data collection and third party use of information policies?**

Public power utilities comply with state and local laws and regulations on customer privacy and data access. Some public power governing bodies have implemented policies and procedures designating consumer information as confidential and establishing rules for third party access to consumer information.

Public power utilities are also addressing cyber security, both in regard to the electric grid and to the communications technologies used throughout a utility's system. (APPA assists its members by participating in the NIST and North American Electric Reliability Corporation ("NERC") processes; by communicating information via list-serves and newsletter and magazine articles; and by providing webinars and other education opportunities.) Public power utilities protect customers' data by implementing effective cyber security plans. Actions taken include using the utility's own, proprietary fiber installation to reduce risk of unauthorized breaches;

ensuring that AMI bidders abide by cyber security and interoperability standards; contracting for wireless networks that use secure transfer protocols; and contracting with specialists to develop cyber security plans that will provide security across all aspects of the utility's operational network.

18) **Should DOE consider consumer data accessibility policies when evaluating future Smart Grid grant applications?**

DOE should not require specific data accessibility provisions as a prerequisite for approving smart grid grant applications. If data access issues are relevant to the proposal, DOE could consider whether the applicant's policies are suitable for the proposed investment and use of the proposed installation.

WHEREFORE, APPA thanks DOE for the opportunity to comment on these important issues and submits these comments for DOE's consideration.

Respectfully submitted,

AMERICAN PUBLIC POWER ASSOCIATION

By **/s/ Diane C. Moody**

Susan N. Kelly, Senior Vice President of Policy Analysis and General Counsel
Diane C. Moody, Director of Statistical Analysis

American Public Power Association
1875 Connecticut Avenue, N.W., Suite 1200
Washington, D.C. 20009-5715

202-467-2900; fax: 202-467-2910
E-mail: skelly@appanet.org
dmoody@appanet.org

July 12, 2010