




**National Rural Electric  
Cooperative Association**

A Touchstone Energy® Cooperative 

July 12, 2010

U.S. Department of Energy  
Office of the General Counsel  
1000 Independence Avenue, SW.  
Room 6A245  
Washington, DC 20585

E-mail: [broadband@hq.doe.gov](mailto:broadband@hq.doe.gov)

**RE: NBP RFI: Data Access**

***Introduction***

The National Rural Electric Cooperative Association (NRECA) is the national service organization representing more than 900 not-for-profit, member-owned rural electric cooperatives (“Cooperatives”). Most of NRECA’s members are distribution cooperatives, providing retail electric service to more than 42 million consumers in 47 states. NRECA members also include approximately 66 generation and transmission (“G&T”) cooperatives that supply wholesale power to their distribution cooperative member-owners. Cooperatives provide service to approximately 75 percent of the nation’s land mass, resulting in a consumer density of just seven consumers per mile of line, significantly less density than that of investor or municipally owned utilities.<sup>1</sup> Both distribution and G&T Cooperatives were formed to provide their members with adequate and reliable electric service at the lowest reasonable cost. In total, kilowatt-hour sales by Cooperatives account for approximately 11 percent of all electric energy sold in the United States.

---

<sup>1</sup> Investor-owned utilities average 34 consumers per mile of electric distribution line and municipally-owned utilities average 47 consumers per mile.

Cooperatives are widely embracing numerous Smart Grid technologies and have been recognized as leaders in integrating advanced grid technologies.<sup>2</sup> For many Cooperatives, advanced metering infrastructure (“AMI”), distribution automation, and software integration are among the Smart Grid technologies that make sense. The operational benefits of AMI and other distribution automation technologies are often greater in rural areas with low population densities. Low density increases the costs of meter reading, outage response, system maintenance, and distribution system losses. Advanced technologies help Cooperatives to address these issues and thus provide real benefits to consumers including lower distribution costs and fewer and shorter outages. Many Cooperatives also expect Smart Grid technologies will help them improve and expand on their existing demand response programs. For example, richer data from AMI allows utilities to better measure and verify the results of load control and better evaluate, shape, and market demand response programs to consumers.

At the same time, Cooperatives recognize that consumers have legitimate concerns regarding their personal privacy when these technologies are deployed. Before there was ever a concept called Smart Grid, utilities have known a variety of personal facts about the consumers they serve. A utility knows a consumer’s monthly energy use, bill payment history, participation in an energy assistance program, telephone numbers (including unlisted numbers), and whether someone in the household uses electricity-dependent medical equipment. Through online and automatic bill payment options, demand response and energy efficiency audit programs, a utility may come to know a consumer’s personal email address, credit card or financial account number, the age and

---

<sup>2</sup> F.E.R.C. Ann. Rep. on the Assessment of Demand Response and Advanced Metering 8 (Dec. 2008), available at: <http://www.ferc.gov/legal/staff-reports/12-08-demand-response.pdf>.

square footage of a consumer's home, the type of heating and cooling systems and major appliances in use, the degree to which a home is weatherized, whether there is a security system, swimming pool, etc. Within an existing framework of state law and their own, internal policies and procedures, Cooperatives, like other electric utilities, have demonstrated their ability to safeguard such consumer data for some time.

The Smart Grid obviously poses challenges regarding the granularity and volume of data as well as new methods for data collection and transmission. However, NRECA believes that existing and well-recognized privacy principles can and should be applied in this new environment. The Department of Energy ("Department") does not need to reinvent the wheel or recommend a federal, "one size fits all" set of mandatory requirements around consumer data access, use and privacy. Instead, the Department can provide information and guidance that will help utilities, State and local policy makers, and consumers make informed decisions that appropriately balance beneficial uses of Smart Grid data with privacy concerns.

NRECA now offers its responses to questions in the Department's RFI, taking some liberties to reframe those questions and raise other points, as invited in the RFI:

***Who Should Have Access to Energy Consumption Data? (Questions 1, 12 and 13)***

A perhaps more helpful starting point for discussion is to address who should have access to energy consumption data rather than who owns the data. Obviously, to provide and appropriately bill a consumer for electricity, the utility must have access to this data. Certain third party service providers used by the utility also will need access to this data. Particularly for smaller utilities, various functions may be outsourced. For

example, a utility may contract with a third party service provider for some or all of the functions associated with customer billing, payment and collection services, which is a common practice among Cooperatives. Similarly, some utilities may outsource or share resources with another utility or other service provider to handle routine or after-hours customer service calls. In such cases, the call service provider needs access to information that allows the provider to appropriately respond to the customer's billing or other questions. Utilities have service agreements in place with these service providers that include provisions addressing data privacy and security.

Utilities may deal with other third parties that do not squarely fit within the more traditional types of "service providers" described above, but that nonetheless would have a legitimate need to access individual consumer data. For instance, a third party staking or engineering firm would need individual customer data in order to most efficiently size transformers, design protection systems, and otherwise structure the distribution system. Similarly, a third party demand response aggregator, acting as an agent for the distribution utility, might need individual customer data to measure and verify the effectiveness of the demand control devices, to dispatch customer-owned generation, or to request that interruptible customers cut load and then confirm that they have done so.

Many of the concerns about consumer privacy relate to which entities beyond the utility and the utility's service providers should have a right of access to energy consumption data, if any, and under what circumstances. In the case of government officials and law enforcement, existing law addresses the extent to which consumers have a protectable right of privacy regarding utility records (e.g., consumption and billing

information).<sup>3</sup> While Smart Grid technology essentially makes it easier to provide access to this data, and the more granular nature of the data may make it more attractive and useful, existing laws addressing the provision of a consumer's energy consumption data to federal, state, or local governments and law enforcement still apply. Generally, utilities are reluctant to release an individual's consumption or billing information absent a subpoena or other official request or the individual's consent.

With regard to third parties other than the utility's service providers, there is no inherent right of access to consumption data. NRECA believes it should be the consumer's choice regarding whether or not consumption data is provided to such third parties. This debate is not unlike the one engaged in during the advent of retail choice, when new market entrants sought data about individual consumers to market competitive energy services. Some new market entrants lobbied aggressively for data that went beyond basic information about consumers. That is, they wanted access to load profiles and other data in order to "cherry pick" the most desirable consumers – usually those with high consumption and a solid payment history. Through stakeholder led processes, uniform data formats and related standards were created to facilitate data sharing with new entrants, but the individual states that had adopted retail choice determined what data would be shared and with whom. Many states adopted standards or a certification process for new market entrants so that utilities had certainty regarding which entities could appropriately receive such data.

---

<sup>3</sup> See, e.g., Kyllo v. United States, 533 U.S. 27,44 (2001) (Finding that police officers' conclusions about illegal marijuana grow operation within the home ...“were at least as indirect as those that might have been inferred from the contents of discarded garbage, ..., or pen register data, ..., or, as in this case, subpoenaed utility records.”) and New Jersey v. Domicz, 907 A.2d 395, 403-404 (N.J. 2006) (“...no state court has interpreted its own constitution to mandate that the police first obtain a warrant to obtain electric utility records. The state courts that have considered the issue have rejected the notion that there is a legitimate expectation of privacy in such records.”)

If the Department feels that it is necessary to answer the question it asked in the RFI: “who owns consumer data,” then NRECA believes that data is owned by the entity by or for whom it is collected. If a consumer installs on their junction box or on individual devices one of the commercially available products to measure, record and analyze their energy usage, the data they collect belongs to them. Similarly, if a utility or its agent purchases and installs an advanced meter in order to collect data required to bill for electric service and to monitor the condition and performance of the distribution system, then the utility owns the data in the same way that it owns the data it collects through its SCADA system. To take any other position raises questions about whether the utility may use the data it collects or share the data with its agents and service providers for basic operational purposes without express permission from each consumer. Those questions would undermine utilities’ ability and incentive to make cost-effective investments in Smart Grid technology and to integrate this technology with their operations.

The issue of ownership need not be resolved before policymakers can answer the separate and more important questions concerning who should have access to the data, for what purposes, and under what conditions. States and other regulators have been able to answer those questions for decades without assigning ownership of the data to either consumers or utilities. Whether consumers should control what information is shared with third parties is a different question, and is one with which States and other relevant retail regulators have long experience. Many regulators adopted policies governing whether, when, and under what conditions utilities may share customer data with third parties during the 1990s in the context of retail competition. It is NRECA’s position that

a protracted debate about ownership should be avoided and instead the discussion be focused on determining policy frameworks regarding access, security and privacy of energy information within which State and other local regulators can make thoughtful decisions.

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

Much of the discussion regarding Smart Grid privacy concerns has centered on energy information pertaining to individual consumers. And that is certainly appropriate. However, NRECA believes that business customers should not be left out of this discourse. Detailed energy information – consumption, usage patterns, etc. – may reveal proprietary business information, or at least information that the business would rather not have widely distributed for a variety of reasons. For example, a business that markets itself as environmentally friendly may wish to keep the actual kilowatt hours used in its manufacturing facility a private matter between the business and its electricity provider.

As noted above, utilities have a great deal of information beyond just the number of kilowatt hours of electricity being used by consumers. This information allows the utility to efficiently and safely operate the electric system as well as provide customers with desired services. Third parties would likely have uses for some of this other data as well. A utility should not be required to act as any third party's "data broker" such that consumer consent can be effectively bypassed. Neither should a utility be forced to disclose information to a third party for purposes other than those for which the utility collected the data. In short, utilities are entitled to certain privacy protections as well.

***What data privacy standards are most relevant to Smart Grid development, deployment and implementation and what, if any, privacy practices should be implemented in protecting energy information? (Questions 3, 7 & 8)***

NRECA believes that the Department should look to existing and well-established privacy principles that can be adapted for the Smart Grid. These standards have been purposefully designed to work across various industries and to address many types of data. First, the International Organization of Economic Cooperation and Development's ("OECD") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data should be considered.<sup>4</sup> The OECD Privacy Guidelines establish eight principles of data protection for protecting privacy that are widely known, understood and applied. These principles are, in relevant part:

1. Collection Limitation – Placing limits on the collection of personal data and requiring that the data be lawfully obtained, and where appropriate, with the knowledge or consent of the individual.
2. Data Quality – Ensuring relevancy of the data for the purposes for which it is to be used, and, as necessary for those purposes, ensuring data accuracy, completeness and currency.
3. Purpose Specification – Providing notification of the purposes for which personal data is being collected, no later than at the time of collection and limiting subsequent use of that data to those purposes or other, compatible purposes.
4. Use Limitation – Limiting disclosure of personal data for purposes other than those specified without prior consent or under authority of law.
5. Security Safeguards – Protecting personal data from unauthorized access, use, modification, disclosure or destruction through the use of reasonable security safeguards.
6. Openness – Operating with transparency about one's practices and policies with

---

<sup>4</sup> See OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), available at [http://www.oecd.org/document/18/0,3343,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html) ("OECD Privacy Guidelines").



respect to personal data.

7. Individual Participation – Ensuring that an individual has the right to: know what data is being collected; reasonable access to that data; challenge data that is incorrect, incomplete, no longer necessary, etc.
8. Accountability – Having accountability for complying with measures which give effect to these principles.

Another set of principles to be considered are those issued by the Department of Homeland Security (“DHS”). DHS’ Fair Information Practice Principles (“FIPPs”) <sup>5</sup> implement DHS’ responsibilities under the Privacy Act of 1974, <sup>6</sup> and have been used as a model in other federal laws and various State laws. While Smart Grid data is distinguishable from the types of personally identifiable information sought to be protected under the Privacy Act, certain Smart Grid data arguably raises the same or similar degree of concern. The DHS FIPPs are: (1) Transparency, (2) Individual Participation, (3) Purpose Specification, (4) Data Minimization, (5) Use Limitation, (6) Data Quality and Integrity, (7) Security, and (8) Accountability and Auditing. In addition, there are the Generally Accepted Privacy Principles (“GAAP”).<sup>7</sup> The ten GAPP principles are: (1) Management; (2) Notice; (3) Choice and consent; (4) Collection; (5) Use, retention and disposal; (6) Access; (7) Disclosure to third parties; (8) Security for Privacy; (9) Quality; and (10) Monitoring and enforcement. In large part, the OECD, GAPP and FIPPs are consistent. This consistency seems to indicate that certain privacy principles are “fundamental.”

---

<sup>5</sup> Privacy Policy Guidance and Memorandum No. 2008-01: *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (Dec. 29, 2008), available at [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_policyguide\\_2008-01.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf).

<sup>6</sup> Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

<sup>7</sup> Available at

<http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/Generally%20Accepted%20Privacy%20Principles.aspx>.

The National Institute for Standards and Technology (“NIST”) in its Second Draft NISTIR 7628, Smart Grid Cyber Security Strategy and Requirements released in February 2010<sup>8</sup> discussed these principles and related them to the Smart Grid. NIST also suggested specific privacy practices to apply the principles. NRECA generally supports NIST’s proposals contained in the Second Draft NISTIR. We offer a somewhat consolidated statement of privacy principles here for consideration:

1. Disclosure – A consumer should be informed about what type of data the Smart Grid technology can capture, for what purposes the data will be used, and the relevant policies and practices of the data collector or user. Ideally, such disclosure should occur before or at the same time as the technology roll out.
2. Data Limitations – Data should not be collected from the consumer unless it is obtained lawfully, used for the disclosed purposes, or used for other uses that the consumer authorizes.
3. Right to Access and Correct – A consumer about whom data is being collected should be provided with reasonable access to the data and have the ability to seek corrections of data that is inaccurate, incomplete or no longer current.
4. Data Sharing – A utility may provide data to its affiliates, agents, and service providers to perform the disclosed purposes, but a consumer’s consent should be required before data is shared with any other third party. A utility should be permitted to recover the reasonable costs incurred to provide data to an authorized third party.
5. Safeguards – Data collectors and users should employ reasonable measures to protect consumer data from unauthorized access, use, modification, disclosure or destruction.
6. Accountability – Data collectors and users should take appropriate steps to ensure that those handling Smart Grid data are held responsible for complying with the privacy principles.

---

<sup>8</sup> Available at <http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7628> (“Second Draft NISTIR”).

Utilities can use privacy principles such as these together with any applicable mandates<sup>9</sup> to devise – or more likely just revisit and revise as necessary – appropriate privacy practices. As noted above, utilities have dealt with privacy and data security issues for some time. In addition to specific state requirements for utility data practices, utilities fall within the scope of other privacy-related laws. For example, 46 states have adopted data breach notification laws, requiring holders of protected data to notify consumers in the event of a security breach.<sup>10</sup> Also, utilities with significant financial activities, such as those that have consumer financing programs for the purchase of electric appliances, heat pumps, etc., trigger Gramm-Leach-Bliley requirements.<sup>11</sup> And, utilities must comply with the Federal Trade Commission’s identity theft prevention “red flag” rules.<sup>12</sup> Given that utilities: may be subject to different privacy requirements by the state in which they operate; may trigger the application of certain laws or regulations based on their specific activities; come in varying sizes; have different organizational structures; and have various types of arrangements with service providers; privacy practices will need to vary somewhat for each utility. As a result, utilities need the flexibility to design appropriate and reasonable privacy practices.

On the other hand, third parties may not be subject to the same types of data privacy-related requirements under which utilities operate. They will likely not have the long history dealing with energy information generally that utilities do. Third parties also would likely not have an established, ongoing relationship with the consumer in the same

---

<sup>9</sup> The Second Draft NISTIR takes note of state level requirements. *See, e.g.*, pp.100, 103 and App. E.

<sup>10</sup> *See*, <http://www.ncsl.org/default.aspx?tabid=13481>.

<sup>11</sup> The Financial Modernization Act of 1999, 15 U.S.C. § 6801-6809. *See* the Federal Trade Commission’s web site for information on the implementing regulations at: <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>.

<sup>12</sup> 16 C.F.R. § 681.2. For more information, *see* <http://www.ftc.gov/redflagsrule>.

way that utilities do. Nor is it likely that third parties would be accountable to a state public utility commission (absent some new requirement) or to a consumer-elected board of directors as Cooperatives are. For these reasons, it merits further discussion regarding whether certain privacy practices should be required of third parties and, if so, how such requirements would be imposed and enforced.

***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? (Question 4)***

It would be very difficult to provide consumers the ability to opt in or out of smart meter deployments. Such deployments require extensive planning, area by area, to ensure continued system availability (the lights staying on) and reliability. Further, utilities are deploying smart meters for a variety of beneficial uses beyond just enhancing the information that can be presented to the consumer, many of which may not be readily apparently or widely understood by consumers at this point in time. The realization of these benefits by all of the utility's consumers would be significantly undermined if some consumers declined to have a smart meter installed. To illustrate, it raises costs for all consumers when a utility must send a meter reader out to only a few residences with analog meters within a large service territory where the rest are smart meters being read remotely. It is also not cost effective for utilities to enter manually a small number of meter readings into its customer information system ("CIS") and billing system when the rest of the utility's meter readings are automatically integrated with the CIS and other systems through a meter data management system ("MDMS"). It can substantially slow outage recovery and increase the cost of responding to outages if differences in meters create blind spots in the utility's outage management system ("OMS") and geographic

information system (“GIS”). Such blind spots can also undermine a utility’s ability to use AMI to reduce distribution system losses, maintain proper voltage and frequency, and perform preventive maintenance.

Allowing consumers a choice in this context would introduce unnecessary burdens and costs in an already challenging process of deploying and integrating AMI with CIS, OMS and other systems. It could also undermine the business case for the investment in the smart meter technology. Uniformity across the entire system, or at least to the extent practicable, or across certain portions of their systems, allows utilities to reduce the cost per meter for acquisition, installation, and integration with other software systems. For these reasons, a determination to provide for a consumer “opt out” should not be entered into lightly. It is NRECA’s belief that consumers’ concerns about smart meters can be addressed most sensibly by building awareness and understanding of the technology’s capabilities and employing fair and reasonable privacy protections. Ultimately, a balance must be struck between consumer privacy and a utility’s obligation to provide safe, reliable and affordable energy to consumers. These determinations should be made by the States or other relevant retail regulators as the bodies that are regularly tasked with such balancing decisions.

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

In NRECA’s opinion, it makes sense to address consumer privacy protections at the outset of designing the Smart Grid security architecture, recognizing that developing a security architecture in tandem with designing the system itself and accompanying engineering processes is a significant challenge. NRECA believes that NIST is taking the

appropriate steps to identify the security architecture needed for the Smart Grid and is doing so in a holistic fashion, including for the purpose of protecting consumer privacy. Indeed, the Second Draft NISTIR<sup>13</sup> builds considerably on the first draft and later versions will address additional matters not included in the second draft. NRECA does not believe it is necessary to replicate a discussion in this forum that is already taking place as part of the NISTIR process.

***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?***  
**(Question 11)**

NRECA applauds the Department for expressing its intent to respect the jurisdiction and expertise of others. Clearly, DOE has an important role to play in advancing Smart Grid policy at the federal level. But, there are others who have roles to play as well. NRECA believes that the Department should continue to do what it has already begun doing – which is to facilitate a productive and inclusive dialog regarding important Smart Grid policy issues. Further, NRECA welcomes DOE’s leadership in the Administration’s cross-departmental Smart Grid subcommittee.

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

If the goal of providing access to Smart Grid energy information is to enable consumers to better manage their energy consumption and/or lower their electric bills, then at a minimum, consumers and third parties that they may authorize, would need information about how much energy they are consuming and what price they are paying

---

<sup>13</sup> *Supra* note 8.

for that electricity. If a utility offers time-varying rates, then consumers should also have access to information that identifies the times at which they are consuming energy and information on the prices charged at different times. To have access to historical consumption information, on a more granular level than is provided in monthly electric bills, would also be useful to consumers to help identify patterns of use.

There is not a single, simple answer to the question of what specific “form” such information should take. Some advocate that the information must be accessible from the Internet, but this ignores a significant group of consumers that lack access to the Internet (particularly broadband access), do not have a computer in the home, or otherwise lack computer literacy. Others want to see data provided in “machine-readable format” so that it can be easily manipulated for display in a variety of electronic devices. At present, no data standards exist, but the Smart Grid Interoperability Panel’s Priority Action Plan #10 to create an “energy usage information model” is a work in progress.<sup>14</sup> NRECA favors a stakeholder process to reach consensus on the form or format such information should take.

NRECA also believes that the decision about whether, when, and in what manner utilities should install the hardware and software required to provide consumers the energy information discussed above should be made locally by States and relevant retail regulators. That decision has significant cost implications for utilities and their consumers. It also depends significantly on the nature of the hardware and software currently in use at the utility, the useful life of that investment, the options available to the utility in light of its location, geography, and available resources, and the needs and

---

<sup>14</sup> See, NIST Smart Grid Collaborative Web Site at: <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP10EnergyUsagetoEMS>.

interests of the utility's consumers. States and other relevant retail regulators are experienced at weighing these kinds of factors, are well positioned to understand the needs and interests of local consumers, and are politically accountable to those consumers.

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

Some believe that the data is only useful if it is provided in “real time,” regardless of genuine issues regarding metering system capabilities, data quality, the costs associated with providing data at such intervals, and level of consumer interest. NRECA does not agree. As eloquently stated by Conrad Eustis, Director of Retail Technology Development, Portland General Electric, on July 1, 2010 in testimony before the Subcommittee on Technology & Innovation, Committee of Science & Technology, of the House of Representatives:<sup>15</sup>

NIST also needs to focus on developing standards and processes that make sense for consumers and addresses consumer behavior. For example, one complex and low priority transaction involves providing “real time” time usage data from the meter to the home display. While desirable for some customers, most of the value in the usage data is available from non-real time sources like a web page with perhaps a day of delay. PGE implemented a home display pilot in 2003. While half the customers found them interesting, most stopped accessing the displays after about a week. Energy is a low involvement product; **effective smart grid implementations in the home will need to emphasize set and forget controls,**

---

<sup>15</sup> Available at <http://science.house.gov/publications/Testimony.aspx?TID=15472>.



**and not depend entirely on real time involvement for their success. Spending time and money on programs consumers do not want should be avoided.**

(Emphasis added.)

Unless a utility has implemented time varying or dynamic pricing, there is really little need for a consumer to have access to energy consumption information in real or near real-time. Further, it should not be assumed that real-time or near real-time prices are necessary to support home energy services. Cooperatives have used non-price-based demand response programs very successfully for more than 30 years to improve service, enhance reliability and lower energy costs for their member-consumers. The tremendous value available to consumers from non-price-based home energy services should be recognized.

***What steps have electric cooperatives taken to implement Smart Grid privacy, data collection and third party use of information policies? (Question 17)***

As noted above, Cooperatives are not new to addressing data handling and privacy matters. Most have policies and procedures in place designed to safeguard consumer data and restrict access by third parties other than their own service providers. A little more than a decade ago, when retail restructuring was underway in about half the states, NRECA encouraged its members to review their policies and practices in light of restructuring, and even developed and distributed a model privacy policy based on the OECD Privacy Principles. NRECA intends to engage in a similar outreach effort to members specifically in the context of the Smart Grid. Given that deployments are still in the early stages, and the dialog is ongoing about what the appropriate data privacy policies should be, NRECA has not yet felt the time is right to begin that effort.

According to NRECA's own research conducted in 2009, approximately half of Cooperatives have begun to deploy AMI to some portion of their service areas. Of those with some AMI deployed, many are still working to fully integrate with other software used by the cooperative, including: CIS (42% completely integrated; 33% partially); GIS (8% completely integrated; 18% partially); and MDMS (13% completely integrated; 9% partially). At the same time, Cooperatives are reaching out to their consumers to identify what expectations they have regarding access to and privacy protections for energy consumption information. In 2009, the more than 700 NRECA members who are Touchstone Energy® Cooperatives conducted a nationwide study of cooperative member interest in energy efficiency information.<sup>16</sup> This research found that members of all ages were interested in receiving a report comparing their homes' energy use to other, similar homes in the area. Younger members (those between 18 and 44 years of age) were very interested in online access to the historical energy use of their homes. Interest among older members for that online access was considerably less. As they gather this information and gain practical experience with the technology in the field, Cooperatives will likely further revise and refine their practices.

NRECA would like to offer a few examples of what Cooperatives are doing now:

- Sawnee EMC (Georgia) – Sawnee is using its corporate web site, printed brochures, and other communications vehicles to explain, in consumer-friendly terms, what AMI data is being collected, how it will be used, and how it will be kept secure.<sup>17</sup>
- Rappahannock Electric Cooperative (Virginia) – Rappahannock is already working to assure its members of the data security measures it is designing into

---

<sup>16</sup> Cooperative Difference research is proprietary. Excerpts here are shared with permission of Touchstone Energy Cooperative, Inc.

<sup>17</sup> See Sawnee EMC's AMI web site at <http://www.sawnee.com/ami/default.aspx>.

its Smart Grid project.<sup>18</sup>

- New Hampshire Electric Cooperative – New Hampshire Electric is embarking on a Smart Grid AMI installation this fall and actively informing members about the technology’s capability and how members’ privacy will be maintained.<sup>19</sup>
- Wright-Hennepin Electric Cooperative (Minnesota) – Wright-Hennepin is using a secure, online platform called “MyMeter” to provide its consumers with access to their daily energy use.<sup>20</sup>

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

Smart Grid technologies are numerous and can be applied at various points of a utility’s system all the way from the site of generation, through transmission and distribution, to the end-use consumer. NRECA does not believe that a grant application should receive a lower priority or evaluation score because the applicant seeks funds for a project that does not reach the end-use consumer. Conversely, a Smart Grid application that seeks funds for technologies deployed at the consumer end should not be automatically given some preference because the application includes consumer data access policies. The merit of any future Smart Grid applications should be judged on the overall benefits of the project relative to its costs, along with any other statutorily mandated evaluation criteria.

***Conclusion:***

The Department of Energy’s efforts to bring together various stakeholders to engage in a productive dialog that seeks consensus on critical policy issues is much

---

<sup>18</sup> See <http://www.myrec.coop/news/news-REC-receives-smart-grid-investment-grant.cfm>.

<sup>19</sup> See <http://www.nhec.com/AMI.php>.

<sup>20</sup> See [http://www.whe.org/Residential\\_Service\\_Center/MyMeter/index.html](http://www.whe.org/Residential_Service_Center/MyMeter/index.html).

needed and to be commended. NRECA appreciates this opportunity to provide comments on the subject of consumer data access, third party use and privacy. Smart Grid technologies have the potential to provide consumers with significant energy and financial savings with corresponding benefits to the environment. These technologies can also deliver a wealth of new, more granular data regarding how various components of the electric grid are functioning, and, as well, information about how and when consumers are using energy in their homes and businesses. Consumers can use this information to better understand, and if they have the desire and ability, to modify their energy use.

Having more and better data on energy consumption and use patterns allows utilities to improve customer service, enhance grid performance, and better integrate new resources and loads. This data also creates new potential business opportunities for companies that want to sell consumers new energy monitoring and management devices, smart appliances, and energy information and management services and applications. Such uses must be appropriately balanced with consumers' legitimate privacy concerns about the use and release of this data. NRECA believes that this balance is best struck on a State and local level. At the same time, having national standards and a national dialog to vet general privacy guidelines and practices is a productive and worthwhile exercise.

Respectfully submitted,

A handwritten signature in black ink, reading "Tracey Steiner". The signature is written in a cursive, flowing style.

Tracey B. Steiner  
Senior Corporate Counsel