DRSG
DEMAND RESPONSE and SMART GRID Coalition

1615 M Street, NW, Suite 900
Washington, DC 20036
www.drsgcoalition.org
202.296.1640

COMMENTS OF THE DEMAND RESPONSE AND SMART GRID COALITION

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

July 12, 2010

The Demand Response and Smart Grid Coalition (DRSG)[1], the trade association for companies that provide products and services in the areas of demand response and smart grid technologies, respectfully submits its comments to the Department of Energy's Request for Information "Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy."

1. Who owns energy consumption data?

DRSG believes that there is a co-ownership of an individual's consumption data between utilities and their customers. The customer owns such data in that they can access it at any time once available from the utility and use it for their own purposes, particularly for energy management. The utility also owns such data in that it requires such data in its operations to serve a given customer and efficiently manage the electric grid, and thus they must be able to access it at anytime.

With respect to aggregate data (e.g. what's recorded by PSUs), we believe it's co-ownership as well: the utility (and or the organized market regional transmission operator) along with the municipality who has hosted the metering unit on its geographic turf.

We do not see the need for grid operators to have a detailed understanding of the devices within the home as this could be construed to be sensitive information. We do not believe that consumer control

[1] Aclara, Advanced Telemetry, Ambient, Amplex, Bridge Energy Group, Boeing, CalAmp, CALMAC, Cisco, Comverge, Conservation Services Group, Cooper Power Systems, Corporate Systems Engineering, CPower, Direct Energy, Echelon, Eka Systems, eMeter, Energy Capital Partners, EnergyConnect, Energy Curtailment Specialists, EnergySolve, EnerNOC, Enfora, EnOcean Alliance, Enspiria Solutions, GE, Google, Honeywell, Ice Energy, Itron, Johnson Controls, KMC Controls, Landis+Gyr, LG Electronics, Lockheed Martin, Lutron Electronics, Oracle, PCN Technology, Sensus, Silver Spring Networks, SmartSynch, Space-Time Insight, Steffes, Tendril, Trilliant Networks, Tropos Networks, Universal Powerline Association, U-SNAP, Whirlpool, ZigBee Alliance, Ziphany

over data within the home impedes the needs of utilities or other parties to obtain and use information needed for their business purposes.

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

Certainly energy consumers should be entitled to a high level of privacy protection. Utilities and other parties must utilize processes, procedures and technologies that ensure that a consumer's data is only accessible to the consumer, the utility and any third party that has been authorized by the consumer to have access. Authorization by the individual is the key: no third party (including those with access to aggregate data, such as the municipality outlined above) should have access to individual consumption or billing information, without the individual's authorization.

The utility owns the use of an individual's information for its operational purposes only (outlined above). Any commercial use of that information ought to be the individual's prerogative. We believe that privacy should be an objective relative to all energy information that is produced by the utility for and/or by the customer. Yet different privacy rules may make sense for different types of information.

DRSG acknowledges that there are established procedures, based on legislation, regulation and court decisions that pertain to the access by law enforcement officials and civil litigants, including obtaining appropriate warrants or court orders. DRSG expects that information related to energy consumption will not be an exception to such. Additionally, the concerns associated with energy information needs to be properly balanced with the magnitude of costs required to ensure privacy protection.

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

Utilities have existing privacy practices and processes for consumer information that stem from their longstanding billing and customer service operations. However, concern is understandably rising as the amount of information to be created and stored increases, and as the communications technologies that are deployed begin to multiply. However, the electricity and utility industry is not the first to encounter these apparent challenges. Banking, telecommunications, internet commerce and many other industries have developed practices that can be looked to for their application to energy and electricity.

Much of this is guided by the Fair Information Practice Principles (FIPPs) put forth by the US Federal Trade Commission. These are 1) notice/awareness 2) choice/consent, 3) access/participation, 4) integrity/security, and 5) enforcement/redress. While these principles are broad, they nevertheless can be used by policymakers, utilities, smart grid companies, and stakeholders to balance the many factors that must be considered as specific practices and policies are being developed relative to energy consumption 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?**

Consumers should not be able to opt out of a smart meter deployment by a utility. Smart meters are part of the modernization of a utility's business operations with an aim of improving efficiencies and reducing costs. The installation of a smart meter at a consumer's premise does not require any new action by the consumer. It does not require that they enroll in any new program or subscribe to any new type of electricity pricing or billing. In fact, based on deployments to date, most consumers do not even know that a smart meter has replaced their old meter. Consumers should not be able to opt out of smart meter deployment any more than they should be able to opt out of the use of a scanner in a supermarket or a new pump at the gas station – other examples of new technology being introduced.

It is true that new information is being created by a smart meter, particularly with respect to interval measurements. Consumers should indeed have control over how and with which third parties this information is shared.

One of the driving principles of the smart grid (which smart metering is an integral part of) is the idea of a grid-wide increase in intelligence and communication. Besides the dramatic increase in cost of a "surgical" deployment versus a system-wide deployment, the lack of smart metering obviates many operational benefits. To cite just one and relatively small example, smart metering at all homes behind a distribution transformer allows the utility to "right size" the transformer, detect trending patterns to increase the size of transformer before it fails or even downsize and reduce costs and better utilize its assets. This doesn't even touch upon the fact that smart metering allows automatic detection of a meter behind the transformer that is potentially lost if people "opt-out". With smart metering coupled with distribution automation, an outage could be restored (self-heal) in a matter of minutes as opposed to waiting to hear from customers and rolling trucks. Customers should, however, be able to opt in/or out of sharing their data with anyone in addition to the utility.

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

It first must be recognized that there are existing mechanisms and channels for consumers to report concerns or problems concerning their electricity service. These include utility customer service operations but also include a state utility commission (or equivalent in the case of some utilities), state attorneys general and official state consumer advocates.

However, it is in the interest of the utility and all of those other parties to recognize that (1) a smart meter deployment requires extra up-front communications/education effort to proactively allay concerns, and (2) special channels and mechanisms for consumers may be warranted that are specific to the smart meter deployment.

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?

Taking the broadband issue first, it must be recognized that limited access to broadband technologies is not a limitation to the deployment of smart metering and other demand response and smart grid technologies and practices. Broadband is but one of the many technology/communications options that can be used.

Low income consumers as well as those with low literacy should be given special consideration in smart grid policies and deployment of smart grid technologies such as smart meters. However, the installation of a smart meter at the home of such consumers does not establish any requirement that such consumers have access to broad band or participate in any new program or any different type of pricing or rate. For the large number of such consumers, the installation of a smart meter will simply be a "swapping out" of one meter for another.

The new smart meter will open up new options for such consumers to manage their electricity bills and lower their costs. Contrary to the statements of many parties, such consumers have been shown to be accepting not only of the new meters but of these new options that they can take advantage of. However – and to state once again – such consumers would not be required to do anything upon installation of a smart meter and their relationship with their electricity provider would continue as before.

State agencies and regulatory bodies have long experience addressing the needs of these communities that should be recognized, considered and included in any new policies and practices developed. Utilities often have outreach campaigns to communities where English is not the first language. Education on a smart meter deployment and any new options that come with that should work through those existing outreach campaigns as well.

Regardless of the target audience, however, it will be important to right up front establish policies and practices on consumer education and communication. Each target audience may have different needs in this respect, but all will benefit from this. In this regard, the National Action Plan on Demand Response offers a new vehicle for support, and DOE and other Federal agencies should support the NAP to the greatest extent possible.

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

DRSG believes that the Fair Information Practice Principles ("FIPPs") provide useful guidelines. As defined by the US Federal Trade Commission, the five FIPPs are notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress. The FIPPs are a useful starting point for developing more concrete privacy policies. They also provide a strong foundation for establishing specific rules, although we recognize that a spectrum of privacy policies will comply with these guiding principles. Therefore, we advise caution against the temptation to believe that the principles will by

themselves generate concrete or specific rules and policies. Rather, industry and policymakers should keep the FIPPs in mind when balancing the many other issues and concerns that are implicit in smart grid policies.

The National Institute of Standards and Technology (NIST) has a task force that is examining this issue in greater detail. Specifically, the Privacy Sub-group of the Cyber Security Coordination Task Group (CSCTG) has taken a broad look at the laws, regulations, and standards relevant to the privacy of information related to consumers' use of electricity.[1] Many of these findings are detailed in the recently released expanded draft of NIST IR-1628.

Attempting to define privacy standards that will be suitable worldwide, however, would be unwise. Privacy is a cultural notion, and cultures differ in the aspects of life that they consider to be private, and the manner in which they seek to safeguard their privacy. Even within the United States, no single regime or law addresses the issue of privacy. Instead, we have privacy provisions in constitutions, privacy laws established in civil and criminal court decisions, and hundreds of discrete statues at the state and federal level.

In addition to FIPPs, other "privacy principles" have been articulated by the U.S. Department of Health Education and Welfare's "Fair Information Practices" (1973) and the Department of Homeland Security's Fair Information Practices (2008). The purposes for data collection included in those principles are:

- Empowering consumers to understand and control their energy use
- Enabling utilities to manage the grid efficiently and economically
- Additional uses of the data (beyond the primary purposes) ought to be permitted only with consumer informed consent
- Consent can be given either on an opt-in or an opt-out basis, as long as the choice is made knowingly
- If the data is sought by law enforcement agencies or civil litigants, well-established bodies of law for collecting individual information should be observed, e.g., the law concerning warrants for criminal investigations
- Utilities and third parties transmitting and/or storing the data should be required to observe data security standards
- These standards should be defined nationally, so that utilities operating in more than one state are not required to observe differing security protocols

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

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?

The core principles of FIPPS provide a well-balance foundation that both conform to consumer expectations, protect their data privacy without inhibiting innovators and their ability to experiment. The United State has long been a leader in innovation because of our ability to adopt comprehensive policies that protect both innovators and consumers. DRSG strongly supports healthy and inclusive privacy policies that require utilities, authorized third parties, and other stakeholders to comply with the reasonable expectations to use data only for specified, authorized purposes.

As noted in responses to question 7, no single data privacy standard fits all needs. "Reasonable expectations" as to what information ought to be private vary from community to community. On the other hand, having varying data requirements in different jurisdictions will thwart rather than promote innovation and experimentation.

The solution is to require a threshold of procedural safeguards, including meaningful disclosure and clear and simple opportunities to give or withhold consent, so that consumers empowered to make meaningful choices about the use of their data. As long as these requisites are in place – information and choice -- privacy interests are protected while leaving room for innovation and creativity.

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?

Utilities have existing privacy practices and processes for consumer information that stem from their longstanding billing and customer service operations. However, concern is understandably rising as the amount of information to be created and stored increases, and as the communications technologies that are deployed begin to multiply. However, the electricity and utility industry is not the first to encounter these apparent challenges. Banking, telecommunications, internet commerce and many other industries have developed practices that can be looked to for their application to energy and electricity.

Key to the success of the mechanisms chosen will be that consumers receive clear, simple, straightforward guidance and instructions on the steps that they must take and the options that are available to them.

We believe that for C&I customers, who are extremely heterogeneous, that individual contract provisions with third parties are most appropriate. C&I customers are used to dealing with other entities through contracts and their unique needs mean that one size will never fit all. However, in the residential sector model mechanisms, developed by NIST, FERC with input from DOE might be appropriate, with actual adoption, adaption and enforcement taking place at the state or utility level.

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

We believe that smart grid technologies can borrow the best security architectures that apply to other areas of commerce that rely on electronic information, including online banking, internet shopping, and wireless communications. Best practices for data encryption, data storage, and data anonymization can be readily applied to the types of data involved in the Smart Grid, including interval data, to protect consumer privacy. We believe that these standards and architectural provisions are being addressed through the NIST and SGIP process. DRSG believes that the best security architecture is one that can balance liability, accountability and enable consumer confidence and expectations, while doing so at a reasonable cost to the utility and its customers

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 is right to acknowledge these other governmental entities, particularly states and localities that have "front-line" responsibility for consumer protection and electricity regulation. However, it does not make sense to have a patch-work system of rules on privacy and consumer access that vary from state to state. DOE, FERC and FCC have a responsibility to seek federal policy and practice that will ensure consistency of policies in these areas while doing so in a collaborative manner with respect to other jurisdictional entities.

Two specific things also come to mind:

a DOE has not historically been seen as focusing on consumers per se, but more on technologies that consumers might use, or on technologies that consumers might benefit from. It may be time for DOE to undertake an organizational effort to create an internal entity whose primary focus is consumers, and the way that they use energy and what policies and actions are necessary to ensure that consumers have someone representing them as DOE programs and practices are developed.

b. DOE should make every effort to robustly support and fund the implementation of the National Action Plan on Demand Response which has recently been sent to Congress by FERC. One of the main components of the National Action Plan is the creation of communications and educational efforts that will help consumers understand and accept the deployment of the smart grid. Such an effort is important in addressing many of the issues put forth in this RFI.

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

Authorized agents of Federal, state and local governments should, we believe, have access to aggregate data, appropriate to their jurisdiction. For example, a state government should have access to statewide aggregate data, in as real-time as that data is available. A municipality should have access to data that

emerges from, for instance, all PSUs (and other aggregate measurement meters) data that is coming from a meter in its territory.

In cases where there are legitimate policy objectives that may be advanced by accessing and using energy information, we believe it is appropriate to establish procedures and guidelines for how government agencies may aggregate and use aggregated information – where such information does not include personal information of an individual consumer.

Laws regulating government access to private data are well established (an example is the Patriot Act. Similarly, many states have statutes with safeguards regulating the state and local government access to private data. We do not believe that a new, separate mechanism is required simply because the data in question is energy consumption data.

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?

DRSG strongly supports giving *customer-authorized* third parties access to consumption data. Consumers should be free to choose services available from an open and transparent marketplace. With informed and explicit consent, we believe that nothing should prevent the third party from accessing the customer's data. We believe this is consistent with the principle that consumers remain the primary locus for control of their own consumption data.

However, while third parties should not have access to data unless the customer designates them, third parties who are contractors to utilities and essential to the utility's reliable delivery of service should have such access. These third parties are really doing the utility's business and should have access to data that the utility can affirmatively justify is essential to the performance of its core objective: reliable delivery of power to the end-user.

Allowing customer-authorized third parties to access consumption data is crucial for realizing one of the principle benefits of the smart grid – providing consumers with information and tools that allow them to optimize their energy consumption, with ensuring benefits to the utility system as a result of their actions. While consumers empowered by the smart grid will be able to take many actions on their own, the number of choices and the effectiveness of the actions taken will be enhanced by the inclusion of expert third parties that operate at the consumers' express direction.

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

Consumers, or a third party that they authorize to act on their behalf, should have access to all data that pertains to the energy usage of that particular customer. That information should include:

a. Information generated by the meter used for measurement by the utility or other party for purposed of billing the customer. Such information will include electricity usage by interval, but in some cases, particularly with C&I meters, may also include peak demand, voltage, frequency, amperage, power factor and power quality parameters.
b. Information generated by other devices deployed by the utility or other party to help control or manage the consumer's energy usage in the business or premise.

c. Information generated on the business or premise by a device installed by the consumer or an authorized third party for purpose of energy measurement or management.

d. Information specific to the consumer that is deposited in and/or created by a utility or third party in a customer's record.

Examples of the type of data that is necessary to implement time-based pricing and demand response programs are the following:

i. Cumulative consumption and relevant interval data
ii. Real-time or instantaneous energy demand
iii. Current retail price
iv. Real-time generation source information (including emissions profile)
v. Relevant wholesale price information
vi. Demand response event notification
vii. Peak-time rebate opportunities.
viii. Customer specific power quality data

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

Consumers should be able to access electricity data that is measured and created by their meter in real- or near real-time. The introduction of such a requirement must recognize that smart meters will generate more information and are likely to be capable of allowing such access in such a time frame, and that such access is difficult if not impossible with some existing meters that have not yet been replaced with a smart meter. Much of this data needs to be received and acted upon in near real time to affect real time pricing markets, demand reduction, power correction, instantaneous energy efficiency, and other grid and consumer usage improvement strategies. Data access at a later time – even within 24 hours – precludes participation in many markets, products, and services that yield substantial energy reduction and efficiency improvements.

In the case of all meters, a process should be established whereby at the request of a consumer, and at the consumer's cost, modifications to an existing meter can be made to allow such access prior to the deployment of a smart meter at the premise.

One must keep in mind that data directly provided in near real time to a customer may have some distinct differences from what is received and stored by a utility. Utilities have expressed their desire to verify data before releasing it, and contend that allowing consumers and third parties direct access to the data would interfere with that verification. First, allowing customers and their third-party designees to have access to raw data from the meter does not prevent the utility from also getting the data and performing whatever verification, estimation and editing ("VEE") that it needs to do for its own purposes. Secondly, requiring VEE first can prevent customers from having access to near real-time data that is essential for making decisions about consumption and demand response in time to have an impact. Raw data from the meter is necessary for making decisions during the day on operations but is not necessarily revenue grade. In the event of a billing dispute, data that has been through the VEE process is likely to be more accurate and that is an appropriate use of the process, but is not needed in near real-time.

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

Many states are taking steps to address these issues and establish appropriate policies. Here are some specific examples of several state proceedings or initiatives that we believe are relevant to this discussion:

- *California Public Utility Commission*: Docket R08-12-009 ("Order Instituting Rulemaking to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's own Motion to Actively Guide Policy in California's Development of a Smart Grid System.")

- *Colorado*: Docket 09I-593EG ("In the matter of the investigation of security and privacy concerns regarding the deployment of smart-grid technology")

- *California, New York, Pennsylvania, Texas*: Each of these states has established statutes or policies to ensure that consumers have access to energy information directly from smart grid technology

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?

DRSG defers to respondents from the Utility sector on this question.

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

The development and deployment of a Smart Grid is not a future event – it is happening now. Over 40 Million Smart Meters will be contracted for by the end of 2010 and 40 million more estimated to be under contract by end of 2012 that is 80 million of the 150million possible US meters. That said, it is also evolving as new technologies continue to be introduced and new policies and standards continue to be implemented. In using federal funds to support smart grid development, it is prudent for DOE to consider a number of different factors in the selection of grant awardees. Consumer access to information is one of those. At the same time, DOE must take care to recognize that it must change its funding policies in a way that matches the pace of other developments.
