



**Response to Request for Information
from the Department of Energy:
Implementing the National Broadband
Plan by Empowering Consumers and the
Smart Grid: Data Access, Third Party
Use, and Privacy**

[FR Doc. 2010–11127]

July 12, 2010

EnerNOC, Inc. (“EnerNOC”) is pleased to provide these comments to the Department of Energy in response to the Request for Information “Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy.” EnerNOC is a provider of demand response and energy efficiency solutions to utilities, Independent System Operators (“ISOs”) and customers in the commercial, industrial and institutional (“CI&I”) sectors. EnerNOC uses near real-time data collected from utility meters at CI&I customers to monitor and coach performance during demand response events as well as to spot excursions outside normal building operating parameters in our SiteSMART energy efficiency service for large buildings.

EnerNOC does not work with residential electric customers so our comments should be viewed through the lens of a provider to the CI&I sectors. Much of the debate about electric data access and privacy has been with sole reference to residential customers. It is important, however, not to forget the needs of the CI&I sector because they consume 61% of the electricity in the U.S., provide the bulk of the demand response capability in the U.S. and yet are a much more heterogeneous sector than the residential sector.¹ They have the ability to use a wider range of types of energy data for a wider range of purposes and therefore need more flexibility. Fortunately, the CI&I sector is in a good position to use existing contract law to enter into arrangements that fit their particular needs, an option that may not be as practical in the residential mass market. That said, EnerNOC’s responses to the questions below will try to address all sectors, except where stated.

(1) Who owns energy consumption data?

Energy consumption data should be owned by the consumer. It is private, personal information akin to credit card expenditures or mortgage payments. Therefore customers are entitled to control how it is used and by whom. Obviously, utilities should have rights to access usage data for the purposes of directly conducting their utility business such as billing, targeting energy efficiency incentives, and interpretation and analysis for system maintenance and upgrade analysis. That said, consumers should be able to share their consumption data with any third party of their choosing. They should be *allowed* to easily share their data but not be *required* to do so.

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

The consumer is entitled to full protection of their energy information, and their energy information should only be used by utilities for direct utility business purposes, unless the customer voluntarily releases it for other purposes to other parties. Similarly, if a customer releases their data to a third party, that third party should only use it for the purposes that the customer intended them to use it.

¹ Energy Information Administration. Retail Sales of Electricity to Ultimate Customers: Total by End-Use Sector, 2009 (Million Kilowatthours/) http://www.eia.doe.gov/cneaf/electricity/epm/table5_1.html.

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

Energy information should be protected using the same consumer mechanisms used for online services such as banking, travel, and shopping. In all of these industries the customer has the right to “opt-out” of information dissemination yet can designate third-parties and/or proxies to receive any or all of their data. Consumer industry standards fit the utility industry reasonably well and are well-understood by consumers and other stakeholders.

(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?

A distinction needs to be made between the ability to opt in/out of smart meter *deployment* and ability to opt in/out of *sharing data*. Consumers should not be able to opt out of smart meter deployments as the information collected by these systems can and will be used for billing and for larger grid operation and maintenance purposes such as service initiation and outage detection. In addition, deployments of smart meters are most cost-effective when all meters are changed at once because of economies of scale. Finally, some benefits of smart meter deployment, such as outage detection, are ineffective unless all customers have the smart meters and those meters are integrated into the utility operations systems.

Information collected through these meters should be available to the utility for direct utility purposes but should only be available to third-parties with explicit consumer permission. A utility should not be able to use the data for purposes other than direct utility purposes without explicit permission as well. For example, a utility should be able to use data from smart grid deployments to improve the operation of their system but should not be able to sell the consumption data to a third party marketing organization without the consent of the consumer.

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

Existing mechanisms for consumer complaints will probably be sufficient, if the proper policies are in place as described above. Consumers should be able to report issues to a utility’s customer service representatives much as they can now regarding a billing or outage issue. In addition, for investor-owned utilities regulated by a Public Utility Commission, consumers can make use of the consumer assistance office and complaint process that all such commissions have if issues cannot be resolved at the utility level. This mechanism should be available for both the protection of meter data quality and accuracy as well as privacy provisions. Again, at the PUC level the mechanism is there, the Commissions just need to set the policies.

(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?

Ownership and protection of energy information should apply to all customers, regardless of their socio-economic status or access to broadband. Utilities need to maintain telephonic customer service capability for those customers that do not have or use broadband. In addition, most utilities have educational campaigns that reach out to customers whose first language is not English. Policies and rules about data access and privacy can be communicated through these same channels.

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

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.² Many of these findings are detailed in the recently released expanded draft of NIST IR-1628.

(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?

See answer to (7) above.

(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?

Standard consumer mechanisms such as password protection of account and meter data allow the consumer to choose the level of protection most appropriate to them. A consumer can choose to share all, some, or no data with retailers and service providers, and the same choice should be given regarding energy information.

² 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

Customers should have the ability to approve the release of meter data to third party service providers, with such release facilitated through electronic approval and prompt processing by utilities.

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

Energy information should be protected using the same consumer mechanisms used for online services such as banking, travel, and shopping.

(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?

The National Institute of Standards and Technology (NIST) and the Federal Energy Regulatory Commission (FERC) have responsibility to develop communication and privacy protocols for the Smart Grid. Having overall guidance from the Federal government on such matters will help ensure consistency within the country without stepping on state prerogatives. DOE can best help this overall goal of consistency by several activities.

First, DOE require that any funding coming from the DOE for smart grid activities, such as Smart Grid Grants, should conform to the protocols and standards developed by NIST and FERC.

Secondly, DOE should 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?

EnerNOC assumes that there may be law enforcement reasons why government agencies would want access to energy consumption data but is not familiar enough with existing laws related to search warrants to make a recommendation.

(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?

Third parties should be able to directly access all forms of consumer energy information available at and/or from a customer's meter so long as that customer gives explicit permission or access for the third-party to do so.

This information should be accessible to the customer, or their designated third party, directly from the utility meter itself via wired or wireless connection using a NIST approved communication standard or protocol. See discussion below in Q. 15 on the importance of getting raw data from the meter in near real-time. Getting the raw data from the meter, as opposed to from the utility data system has some security advantages as well. First, physical access to the meter in the case of a wired connection can be controlled by the customer and they can grant it to the third party they want to deal with and withhold from others. Second, in the case of a wireless read out, such as the Zigbee standard, proximity to the meter is required and often a code, similar to the one used on home Wi-Fi networks is required to be able to read the data. Finally, no connection to the larger utility system is required, i.e. no log-in to some utility owned program that could be hacked.

Handling and protection of data by third parties should be through a direct agreement between the consumer and the third-party. Standard commercial agreements provide legally- and business-accepted practices and the particulars of such agreements should be set in the commercial market to allow for flexibility and best practices that enhance, not hamper, innovation, the development of new energy efficiency and control applications and the ability of customers to get the most out of their energy use. Third parties should only use the data for the reasons stated in the agreement with the customer, just as utilities should.

This is an area where the needs of the CI&I sector, and the residential sector may differ. CI&I customers are larger and generally used to dealing with contracts for a variety of purposes. Moreover, the heterogeneity of the CI&I market calls for customization. It is possible that standard terms and conditions for residential customers to both share, or choose not to share, their data would be a benefit to them. Such standard terms and conditions would probably best be developed in a “model” at the national level but then adopted and adapted at the state level.

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

Consumers and third parties should have access to all data collected by a utility meter at the point of metering. Standard residential smart meters typically include consumption by interval. CI&I metering often collects more information such as peak demand, voltage, amperage, power factor, and basic power quality parameters. If a meter is capable of collecting a parameter this data should be available to consumers and their third party designees directly from the meter.

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. This is a red herring. 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. (See Q. 15 below on the importance of near real-time data.) 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.

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

Consumers who request it should have access to all data captured by the meter in near real-time, at the shortest intervals the meter can count. 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, such as 24 hours, precludes participation in many markets, products, and services that yield substantial energy reduction and efficiency improvements. Even a delay of one hour on data access can prevent participation in these programs.

Today, EnerNOC is reading the usage of over 7000 CI&I customers in near real-time through the internet. The reason for this is that EnerNOC has commitments of thousands of MWs to different utilities and ISOs to drop load through demand response. By monitoring the customers' usage in near real-time, EnerNOC can see which customers are responding to a DR event, identify the underperformers and coach them to hit their commitment. This makes DR more predictable and consistent for our utility and ISO customers. Getting this same data with even an hour delay (much less a 24 hour delay) would severely hamper our ability to ensure performance.

Currently, the way EnerNOC gets access to near real-time data is by requesting, and paying for, the utility to send a truck out to a customer's premises and install a physical wire output ("KYZ pulse output") on each meter. This can take up to 12 weeks for installation after the customer requests it because utilities are not set up to do mass installations of this type. To ensure that customers and their third parties have access to interval data on a basis other than is used by the utility for billing purposes, utilities will need to specify local outputs for their smart meters before deployment. It is a lot cheaper and faster to have the output installed at the factory when the meter is built. A separate channel can be set aside to provide the customer read-only access to its usage and other data recorded by the meter. The meter information can be sent from the meter to devices within the customer premises via wires or wireless communication protocols such as Zigbee. The type of output and the format of the data should be consistent with NIST designated standards in a machine-readable language.

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

State Commissions, or the National Association of Regulatory Utility Commissioners ("NARUC"), are probably in a better position to answer this question definitively.

(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?

Utility respondents are probably in the best position to answer this question.

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

The DOE should absolutely consider data accessibility policies when evaluating Smart Grid applications. Specifically, all Smart Grid meter deployments should be required to allow data to be available in an actionable timeframe (i.e. near real time) and format (using a common standard and over a common wired or wireless connection that conforms to NIST standards), and all Smart Grid rollouts – regardless of grant status – must include data accessibility, with reasonable and common privacy considerations, as a prerequisite for deployment.

Thank you for providing the opportunity to comment on these important matters. If the Department has additional questions they should be directed to:

Rick Counihan
V.P. Regulatory Affairs
EnerNOC, Inc.
400 8th St., NW, #804
Washington DC 20004
415.517.1861
rcounihan@enernoc.com