701 Pennsylvania Avenue, N.W.
Washington, D.C. 20004-2696
Telephone 202-508-5615
Fax 202-508-5673
www.eei.org

EDISON ELECTRIC INSTITUTE

July 12, 2010

U.S. Department of Energy
Office of the General Counsel
ATTN: NBP RFI: Data Access
1000 Independence Avenue, SW
Room 6A245
Washington, DC 20585

Re: DOE Request for Information – Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy

The Edison Electric Institute ("EEI"), on behalf of its member companies, hereby submits the following comments in response to the request by the Department of Energy ("DOE" or "Department") for information on state efforts to enact Smart Grid privacy and data collection policies; utility practices and policies regarding data access and collection; third party access to detailed energy information; the role of the consumer in balancing benefits of data access and privacy; and policies and practices that should

guide policymakers in determining who can access consumer energy information and under what conditions.[1]

EEI is an association of the United States investor-owned electric utilities and industry associates worldwide. Its U.S. members serve almost 95 percent of all customers served by the shareholder-owned segment of the U.S. industry, about 70 percent of all electricity customers, and generate about 70 percent of the electricity delivered in the U.S. EEI frequently represents its U.S. members before Federal agencies, courts, and Congress in matters of common concern, and has filed comments before the Commission in various proceedings affecting interests of its members.

EEI's members may be directly and indirectly affected by the instant proceeding, as users of broadband communications networks and services. The primary interest of EEI's members in this proceeding is the advancement of policies that promote Smart Grid use and development and ensure that energy data is properly collected, reported, managed, shared and disclosed in ways that are lawful and transparent to consumers, and that are consistent with the core responsibilities of EEI's members to prove safe and reliable electric service.

EXECUTIVE SUMMARY

The electric industry supports the Department's efforts to collect information about energy data access, use and privacy practices and policies for consumers, utilities and others, and appreciates this opportunity to express its views and experiences. EEI's members stand for the rights and privacies of our customers, and recognize that

[1] *See* NBP RFI: Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use and Privacy, 75 FR 26,203, May 11, 2010 ("Notice").

preserving customer trust is essential to our success and to the success of third parties.[2] A thorough understanding of Smart Grid privacy issues and implementation of policies to address these issues is critical to safeguarding customer rights and maintaining a culture of trust between electric utilities and customers.

Protecting customer privacy is an important and well-established priority for EEI's members, virtually all of whom have policies in place to protect access to and use of customer-specific energy usage data ("CEUD").[3] The deployment of Smart Grid technology introduces new data collection and information sharing abilities related to customer energy usage, and raises significant privacy and data access issues, requiring electric utilities to update their policies and procedures. EEI's members are committed to protecting customer privacies, and are working diligently to ensure that our policies and procedures address new and emerging privacy issues.

As the Smart Grid evolves, strong data access and privacy policies are needed to protect against unauthorized access and use of CEUD. EEI's members are concerned that to the extent CEUD leaves utilities' systems and is communicated to the customer side of the meter, utilities and state commissions will lose control over what happens to that data and how it is handled, to the detriment of customers. Third parties face strong incentives to capitalize on the value of CEUD, which in many ways directly conflicts with the interests of utility customer and the efforts of utilities and states to protect that information. Therefore, in order for third parties to gain access to CEUD, third parties should be required to fully disclose to customers how their CEUD will be used and

[2] "Third Parties" are those parties not under contractual obligations with an electric utility to keep customer information confidential and who, therefore, require customer consent to receive such information.
[3] "Customer Specific Energy Usage Data" includes all data specific to an individual customer's energy use (*i.e.*, total and time-differentiated energy and capacity use).

should be responsible for protecting this information. Broad third party access to CEUD without standards or consequences could violate customer trust, which would be harmful first and foremost to consumers as well as to utilities who have worked to gain that trust and taken considerable steps to preserve customer privacy.

Finally, while utilities can and will take proactive steps to implement policies and procedures safeguarding CEUD, customers must be educated to understand the new privacy exposures presented by Smart Grid and be empowered to take steps to protect their privacy.

COMMENTS

1. Energy Consumption Data Ownership

In Question 1, DOE asks who owns energy consumption data?

Ownership of energy consumption data is a complex question that extends beyond a simplistic notion of "ownership," and pertains more to issues of data access and usage. Data ownership is traditionally governed by state law and varies on a state-by-state basis based on different state regulatory structures. Certain states (*e.g.*, Ohio, Pennsylvania, Texas), which allow customer choice in service providers for various "unbundled" service options, require competitive providers to meet state criteria for access to customer energy information collected at the meter, while others retain a vertically integrated utility structure. Different regulatory structures raise different issues of information ownership. The concept of energy usage data ownership is further complicated due to differing utility business models in different states.

Based on state regulatory structures, utility business models, the nature of the relationship between a utility and its customer, and the nature of the energy usage data

itself, there are differing interests in consumption data. Energy usage data is the direct result of a contractual relationship between a utility and a customer based on the provision of energy service, and the interests between these parties must be fairly balanced. On one hand, energy usage data is initially collected by utilities who invest in infrastructure to deliver energy services to a customer, and utilities have, by statute, regulation or practice ownership interests in detailed electricity usage data resulting from this relationship. Parties who undertake the risk of providing capital necessary to capture and manage energy usage data should have rights to the economic value of that data. Similarly, utilities incur ongoing operating costs to transmit, manage and verify energy data. By enhancing and validating this data, utilities derive ownership rights to enhanced and validated CEUD as well as aggregated non-customer specific energy usage data. Customers, on the other hand, have privacy rights associated with their individual CEUD.

Given that the question of data ownership is complex and varies considerably based on numerous factors, an approach to Smart Grid data access based on property rights and ownership interests in energy usage data is problematic and will complicate DOE, Federal and state agency efforts to develop a framework for Smart Grid data access policies.

The critical policy issue for Smart Grid development is not ownership of consumption data, but access to, usage and disclosure of that data. To this end, as the Department has acknowledged, the role of the states in developing data access and privacy standards cannot be overlooked. Specifically, states have jurisdiction over the overall relationship between the utility and the retail customer out of which this data arises. Traditionally, privacy regulation of customer data has been the responsibility of

the states, which have developed various privacy protection laws for customer data. States also have consumer protection laws safeguarding interests of energy consumers. Under these and similar laws, information is furnished directly from consumers to utilities in confidence, and it is well established that the public interest requires maintaining the privacy of that information. Currently, virtually all electric utilities have their own data privacy policies in accordance with regulations promulgated by state regulatory authorities.

Regardless of who owns the consumption data, as a matter of policy utility customers should have access to CEUD reflecting the electric service they take, with that data being provided by utilities through accepted and secure methods of data transportation, using reasonable methods that are technically feasible for the utility. Consistent with applicable state regulations, customers should be able to choose to share their CEUD with third parties, or request that their utility share this information to participate in utility or third party programs. The frequency and manner of providing access to CEUD should be developed between utilities and their applicable state regulatory agencies, since these elements of CEUD access must account for the rate design and other factors within a particular market area.

Notwithstanding a customer's ability to chose to disclose certain CEUD, as discussed above, utilities must continue to have access to and control over all CEUD, including operational data,[4] to effectively render services, maintain safety and reliability, properly and timely bill customers for those services, and for the more general purpose of

[4] "Operational Data" includes data related to the operation of electric utility systems that is not customer-specific, but that includes aggregated customer energy usage data.

providing the best and most innovative services available in order to meet consumer needs. Unlike third-party service providers, the legally-mandated purpose of a public utility is to give reasonable and adequate service. In order to meet these obligations, electric utilities must have full access to individual CEUD.

With further regard to questions on access and usage of CEUD, it is important to recognize that utilities use energy consumption data as part of the *quid pro quo* for the provision of energy services, and it is necessary for the reliable and safe operation of the transmission grid. To this end, utilities should not be required to pay for use of energy consumption data because these legitimate costs would be added to consumer bills, and would introduce additional costs to the provision of electric service, which would be contrary to the public interest. It is critical for utilities to have access to individual CEUD, as it is needed for reliability purposes, to ensure a utility can adequately meet daily and seasonal peak loads. Similarly, utilities must have access to CEUD for billing purposes (*i.e.*, to properly bill customers for services rendered and to effectively respond to billing inquiries). Data access by utilities in these instances is similar to the ability of regional bell operating companies ("RBOCs") to access customer proprietary network information ("CPNI").[5]

---

[5] CPNI means:

> (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and
> (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;
> except that such term does not include subscriber list information.
> *See* 47 C.F.R. § 64.2003(g).

Pursuant to FCC rules, RBOCs "may use disclose, or permit access to CPNI for the purpose of providing […] service offerings among the categories of service […] to which the customer already subscribes from the same carrier, without customer approval." 47 C.F.R. § 64.2005(a)

Moreover, where customers own distributed resources such as on-site generation or storage, or on-site demand response capabilities, utilities require CEUD to ensure safety for customers and for utility employees, to properly bill customers for standby service, to provide net metering, and to validate demand response performance for purposes of administering incentive payments.

2. Privacy Protections for Energy Information

In Question 2, DOE asks who should be entitled to privacy protections relating to energy information?

Both residential and non-residential utility customers are entitled to certain privacy protections related to their individual CEUD, as safeguarded under state consumer protection and privacy protection statutes. Privacy protection of energy information is further mandated by state codes of conduct for utility practices.

Retail customers are entitled to have their utilities maintain the confidentiality of their account records, including information supplied voluntarily by customers to establish service and information related to the utility's supply of energy service as measured by the utility's meter. If customers wish to maintain the privacy of data produced by customer-supplied devices and appliances within their premises, they can undertake such privacy measures as are appropriate for those purposes.

As discussed above, utility customers must have confidence that their CEUD will not be released to third parties without those customers' express approval. Utilities have a long history of protecting customer information, including CEUD, and maintaining protections of sensitive information is critical for continued customer satisfaction, both

for utilities and for third party Smart Grid providers. A recent consumer survey conducted for EEI confirms this, indicating that 46 percent of respondents believe it is "very important" that their electricity usage be kept confidential, 29 percent believe it is "somewhat important," and 79 percent believe only customers and utilities should have access to smart meter information.[6] Further, where the end-user is a commercial or industrial customer, as opposed to a residential consumer, confidentiality of energy usage information is critical, so as to avoid potential competitive harm that might arise from the unauthorized dissemination of energy consumption and cost information. For these reasons, customer privacy of energy information must be adequately protected.

In addition, utilities, as businesses, are legally entitled to certain privacy protections which extend to, among other things, proprietary data such as CEUD which has been enhanced and validated by the utility for internal purposes, as well as aggregated non-customer specific energy usage data. Further, utility privacy protections extend to technical functions of meters and supporting communication infrastructure deployed by a particular utility. These are utility "back office" functions that enable utilities to access meter data remotely, to provide outage indications to a utility, to allow power quality monitoring and detection of meter tampering, and to allow utilities to connect and disconnect certain meters remotely.

Privacy protections must be considered for more general consumer information and data that may be generated, not only by smart meters, but also by Home Area Networks ("HANs") and devices connected directly for third party access. Devices in a customer's premises, which may be potentially connected to HANs, meters, and the

[6] Edison Electric Institute, *Public Opinion On Customers' Information Privacy*, June 9, 2010.

internet, raise additional concerns for consumers, regulators and utilities. In all cases, however, the need for protecting retail consumer and utility privacies must be carefully balanced with the need for promoting innovation of technology.

In addition to consumer access policies, retail customer and utility privacy protections require procedures to ensure that CEUD and other proprietary information are properly disclosed to *authorized* third parties. Verification procedures for authorizing third parties will make certain that only appropriately qualified third parties are capable of obtaining (subject to customer consent) energy usage data. EEI urges the states in considering third party verification procedures, and the Department, in developing guidance for the states, to consider the rules established by the Federal Communications Commission's ("FCC") addressing third party authorization requirements prior to receipt of proprietary information.[7] Notably, the FCC rules set forth specific methods for third party verification (*i.e*., automated systems; conference calls); processes for initiation of third party verification; and requirements for content and format of third party verification. The FCC also establishes language requirements for verification, as well as records retention requirements. Prior to consenting to disclose CEUD, customers should be provided with educational information, such as an explanation of the details of possible information that could be provided to a third party after customer authorization.

In addition to developing guidance for the states, there remains a role for Federal departments and agencies in conjunction with the states to develop privacy practices and controls for the flow of energy usage data across state lines. This flow of information presents a unique set of jurisdictional and practical issues well suited for Federal

[7] *See* 47 C.F.R. § 64.1120 (c)(3).

guidance to the states. Federal departments and agencies should consider developing guidance for validating third parties who have been authorized by the states through individual state certification procedures. Customers and electric utilities would benefit from a consistent method for state-certified third parties to prove the validity of their state authorizations. Consistent procedures are necessary to protect customer privacies from what will likely be many new third party entrants. EEI urges the Department to consider as a model the FCC's rules governing access to CPNI and third party verification, as well as recommendations from the Department of Commerce's National Institute of Standards and Technologies ("NIST") on authentication and authorization of Smart Grid devices and users.[8] As previously stated, however, the need for protecting privacies must be carefully balanced with the need for promoting development of innovative technology.

3. Privacy Practices For Protection of Energy Information

In Question 3, DOE asks what, if any, privacy practices should be implemented in protecting energy information?

EEI urges the Department to proceed carefully in developing guidance as to privacy practices to protect energy information. Smart Grid technology is new and evolving, and it is premature to decide what privacy practices should be implemented to protect consumer information. Any privacy practices must be sufficiently transparent for customers, utilities and third parties, and must facilitate, rather than impede, Smart Grid development. Further, utilities have a strong track record of safeguarding the privacies

[8] *See* NIST report *Smart Grid Cyber Security Strategy and Requirements* ("NISTIR 7628"), Chapter 1 ("Cyber Security Strategy"); Chapter 6 ("Research And Development Themes For Cyber Security In The Smart Grid") (subsections 6.4 and 6.6 address security and survivability architecture of the Smart Grid, and other Smart Grid security issues, respectively); Appendix D ("Bottom-Up Security Analysis Of The Smart Grid") (February 2010).

and energy usage information of their customers based on existing practices and regulatory structures. Absent clear evidence of neglect or abuse by utilities in protecting customer electronic data, there is no rational reason for the DOE to attempt to establish specific standards to protect energy information.

Several important considerations must be taken into account by utilities and regulators prior to developing privacy practices to protect consumer and utility information. As a fundamental matter, and consistent with applicable laws and regulations, utility customers should be able to easily and efficiently access CEUD from their electric utility reflecting the energy services they receive. Such right of access should be incorporated into customers' terms and conditions of service as developed by individual utilities pursuant to state regulatory requirements.

In addition, different retail utility customers will have different privacy needs. Some residential customers will be more sensitive about providing CEUD to third parties and will demand greater privacy protections. Other residential customers will be more amenable to providing CEUD to third parties to take advantage of one or more third party Smart Grid applications and services. Similarly, the privacy needs of non-residential (*i.e.*, commercial and industrial) customers will differ based on the nature and size of their businesses. Non-residential customers may require confidentiality of energy usage information so as to avoid any potential competitive harm that might come from the unauthorized dissemination of energy consumption and cost information. In all instances, energy usage information from smart meters should only be shared with third parties with customer consent, and through accepted and secure methods of data transportation.

Further, different types of data will require different privacy practices and standards, and may be subject to different regulations at the Federal Trade Commission ("FTC") and other agencies. NIST is currently examining how different types of data are being treated by various parties, including regulatory agencies and industry stakeholders.[9] Access to certain types of data and related custodial duties must also be consistent. For these reasons, a clear definition of "data" as it relates to "energy consumption data" must be established. EEI encourages the Department and state regulatory authorities to consider NIST's guidance and recommendations on these issues so as to avoid developing definitions or standards that might be inconsistent with other data treatment practices.

The "front line" for energy information and privacy protection is at the utility level, where energy usage data is collected and used by utilities to carry out their core business of safely and reliably providing energy services. EEI believes that utilities act responsibly with data storage and access, and do so under state regulations as well as corporate governance requirements of the Securities and Exchange Commission and Sarbanes-Oxley. The Department should consider these and similar requirements.

Nonetheless, certain protections must be established at the utility level to safeguard the privacies and energy usage information of electric utility customers. Notably, comprehensive protections for use of CEUD must be established, as well as safeguards on disclosure of CEUD. As noted above, energy usage information from smart meters should only be shared with third parties with customer consent, and through accepted and secure methods of data transportation. Utilities should have clear and

[9] *See* NISTIR 7628.

defined policies for treatment of CEUD that are available to utility customers. Utilities should also protect against loss, theft and unauthorized access of CEUD, and should not release CEUD to third parties absent affirmative customer authorization. Third parties with customer authorization to receive CEUD should be required to obtain explicit customer approval prior to reselling or distributing that data. All privacy protections must follow CEUD, and authorized third parties must be responsible for protecting that data and liable for any unauthorized access or intellectual property infringement that may occur.

Utilities should implement monitoring and compliance programs, consistent with applicable regulatory requirements, to ensure compliance with data policies, and assign privacy responsibilities to appropriate personnel with sufficient authority to ensure that data policies are documented, adhered to and updated from time-to-time as needed, and that internal awareness activities are conducted. Given consumers' interest in the privacy of CEUD, third party service providers must be subject to similar obligations to ensure consistency in privacy protections for this information.

As noted above, state regulatory agencies should consider developing consistent procedures for third parties verifications. Verification of third parties is critical, as are clear policies for obtaining customer authorization for release of CEUD to authorized third parties. To this end, EEI urges the states to consider the FCC's rules addressing these issues. In particular, FCC rules establish safeguards for use of customer-specific information including, among other things, records retention requirements for all CPNI

third party disclosures.[10] Further, FCC rules mandate safeguards against unauthorized disclosure of CPNI, and require that telecommunications carriers take "reasonable measures" to discover and protect against unauthorized disclosures.[11] The FCC also details procedures for notifying law enforcement in the event of unauthorized access to CPNI.[12]

4. Consumer Ability to Opt-In/Out of Smart Meter Deployment, and Ability to Control Information Shared with Utilities or Third Parties

In Question 4, DOE asks if consumers should be able to opt in/opt out of smart meter deployment or have control over what information is shared with utilities or third parties?

For practical reasons, utilities must have control over their deployment of their infrastructure. Allowing consumers to opt out would create "data holes," as well as meter data management systems operational and integration problems, and would significantly hinder electric utility efficiency in deploying smart meters and utilizing Smart Grid technology, in turn raising costs to consumers. Moreover, service reliability could be adversely affected since the existence of "data holes" would diminish the ability of utilities to manage supply and load. For these financial and operational reasons, meter deployments have always been managed between utilities and state regulators. Whatever may be the perceived benefits of providing the ability for individual customers to opt

[10] *See* 47 C.F.R. § 64.2009. The FCC requires records of disclosure or access to be kept for a minimum of one year, and contain specific information. 47 C.F.R. § 64.2009(c).

[11] *See* 47 C.F.R. § 64.2010. The FCC further requires that telecommunications properly authenticate a customer prior to disclosing CPNI to that customer. 47 C.F.R. § 64.2010(a).

[12] *See* 47 C.F.R. § 64.2011.

in/opt out of smart meter deployments, they cannot outweigh these adverse financial and operational impacts that would be felt by all retail electric customers.

Saturation deployment of smart meters is a "win-win" scenario for customers. On the one hand, all customers will receive the benefits from network modernization afforded by deployment of Smart Grid technology. In the short run, these benefits (*i.e.*, improved power quality, increased reliability, increased safety, faster service restoration, increased utility productivity) will be the most significant for consumers. On the other hand, individual customers are under no obligation to subscribe to Smart Grid services (*i.e.*, demand response) for which they may have no need or desire. Therefore, while utilities must have control over deployment of their smart meter infrastructure or hardware, customers should be able to opt out of optional Smart Grid services.

Fundamental to the provision of electric service is that customers must share metered consumption data with utilities. Utility access to individual CEUD is required for proper utility billing, as well as for reliability, safety and compliance purposes. Therefore, a customer should not be permitted to opt-out of sharing CEUD or other consumption data with their utility. Similarly, utilities should not be required to obtain customer approval for use of this data in their provision of energy services. As discussed above, utilities must continue to have access and control over all CEUD, including operational data, to effectively render services and for the more general purpose of providing the best and most innovative services available in order to meet the needs of

the consumer. This limited approach to use of consumption data without customer approval is consistent with FCC rules for usage of CPNI by RBOCs.[13]

Customers should nonetheless be able to opt into sharing of certain other information with utilities or third parties. Namely, customers should have the right not to disclose disaggregated appliance-level data with utilities or third parties, as well as information concerning geographic usage patterns of electric vehicles they drive. In these instances, an “opt-in” approval process for information sharing with third parties represents the best and most effective approach for protecting customer privacy interests, as opposed to an “opt-out” process. Any "opt-in" or "opt-out" process established must be consistent with applicable state affiliate rules.

5. Customer Mechanisms to Report Smart Meter Concerns or Problems

In Question 5, DOE asks what mechanisms should be made available to consumers to report concerns or problems with the smart meters?

Consumer concerns or problems involving smart meters can be addressed through standard customer service practices already employed by utilities, most of which are prescribed by state-mandated complaint-handling procedures and regulations. These processes are employed by every EEI member today, and have been since the inception of electric service. Mechanisms typically available to customers include a variety of communication media methods, including phone, mail and internet-based communications (*i.e.*, email, web-site postings). As utilities expand their

[13] Pursuant to FCC rules, RBOCs "may use disclose, or permit access to CPNI for the purpose of providing […] service offerings among the categories of service […] to which the customer already subscribes from the same carrier, without customer approval." 47 C.F.R. § 64.2005(a)

communications to include newer technologies, these mechanisms may also be used by customers to raise smart meter issues or other utility service issues.

Third parties wishing to access CEUD should at a minimum be made to adhere to all relevant state procedures and regulations, and develop comprehensive customer service practices. Consumers should be able to review and correct personal information. Utilities should establish procedures that allow consumers to review and correct such smart meter data. This principle applies to more than just smart meter data: where the utility holds other customer-specific data, customers should be able to review and correct that data as needed.

6. Policies and Practices Addressing Needs of Different Communities, Including Low-Income Rate Payers

In Question 6, DOE asks how 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?

Given that electric utility data policies and practices are applicable to all communities and customer classes, and protect all consumers equally, there is no significant need to develop policies or practices specific to any one customer class, so long as data policies implemented extend necessary protections to all consumers. The Smart Grid in itself does not impact low-income customers any differently than it does other customer groups. Further, all consumers, including low-income consumers, will benefit from the optimized management of electricity demand and from increased reliability and capacity of the grid, which will be realized through implementation of Smart Grid technologies.

Benefits resulting from network optimization can only be delivered to consumers by their electric utilities, and it is critical that no policies be implemented that would discourage or hamper utility investment in Smart Grid technologies. Moreover, it is important to ensure that all customers have access to these Smart Grid technologies.

Specific to customer access to smart meter data, utilities recognize that customers must be educated about types of information that may be generated by smart meters, and the types of goods or services that may be available to help customers understand and manage energy usage that will be available because of that information. Utility customer education efforts, available to all customer classes, should be implemented in commonly-used languages in a utility's service territory, and in terms understandable to customers. For customers without home access to a computer or the internet, free internet access may be available at public libraries, enabling customers to obtain information about Smart Grid benefits, education about the availability of goods and services that may make use of information derived from smart meters, as well as details of their home energy usage provided by their local utility or metering authority.

7. Data Privacy Standards of Relevance to Smart Grid Deployment

In Question 7, DOE asks which, if any, international, Federal, or State data privacy standards are most relevant to Smart Grid development, deployment, and implementation?

As noted above, privacy regulation of customer data has traditionally been the responsibility of the states, which have developed various data privacy protection, access and disclosure laws and regulations for CEUD as well as other customer information.

States also have consumer protection laws safeguarding the interests of energy consumers.

Pursuant to the Energy Independence and Security Act of 2007, NIST is evaluating existing privacy standards, principles and practices, and new privacy exposures which may be created in Smart Grid environments, and identifying best practices for meeting these new exposures. The results of this effort will be documented in Chapter 3 ("Privacy and the Smart Grid") of NISTIR 7628 ("NISTIR 7628 Privacy Chapter"). Although not standards, the recommendations contained in the NISTIR 7628 Privacy Chapter are highly relevant to Smart Grid development. The NISTIR 7628 Privacy Chapter provides a useful reference for utilities, policy makers and third parties as they update existing privacy policies and practices - provided that users remain cost conscious and use good judgment in deciding how to implement relevant recommendations in a cost-effective manner. Briefly, the NISTIR 7628 Privacy Chapter recommends the following:

(1) Conduct a privacy impact assessment ("PIA") upon making the decision to deploy and/or participate in the Smart Grid to identify privacy risks/exposures. Update the PIA whenever major changes may affect privacy;

(2) Develop and document formal privacy policies to:

   a. Assign staff responsible for privacy policy implementation;

   b. Notify customers, before data collection, what data is being collected and how it will be used;

   c. Describe to customers their choices in collection and use of their data;

   d. Ensure that only data necessary for purposes indicated in the customer notification is collected;

   e. Ensure that customer information is only used for the purposes it was collected, only retained as long as needed for those purposes, and is not shared with other parties without explicit customer consent;

f. Ensure customers' ability to access, update and correct their own data;

g. Ensure that customer-specific information is protected from loss, theft, unauthorized access, inappropriate disclosure, etc.;

(3) Employ privacy use cases to address identified exposures or problems;

(4) Educate consumers about privacy exposures and privacy protection options;

(5) Share among utilities and commissions solutions to common privacy problems; and

(6) Limit data collection by smart appliances and other devices to only data needed for purposes of smart device operation.

These recommendations are useful, and coordination of standards between utilities, state regulators, federal agencies and any other various parties is critical for successful implementation of Smart Grid data privacy standards. Further, transparency is needed in this process to assist utilities in preparing for Smart Grid deployment. Going forward, privacy issues should be addressed in a way that balances the need for data privacy with utility obligations to serve customers safely and reliably, to operate the power system, and to perform required system planning functions.

8. Data Privacy Standards Best Suited to Provide A Framework for Opportunities to Experiment, Rewards for Successful Innovators and Flexible Protections

In Question 8, DOE asks 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?

As highlighted throughout these comments, the need for protecting retail consumer and utility privacies must be carefully balanced with the need for promoting innovation of technology. In addition, all privacy practices adopted or recommended

must be sufficiently transparent for customers, utilities and third parties, and must facilitate, rather than impede, Smart Grid development and utility operation and planning.

As noted in our response to Question 7, the NIST Interoperability Standards development process is considering a variety of national and international principles, best practices and standards for meeting new Smart Grid privacy exposures. As part of this open and transparent process, NIST and stakeholders are evaluating potentially relevant data privacy standards that provide flexible protections capable of accommodating widely varying reasonable consumer expectations. The NISTIR 7628 Privacy Chapter provides a useful framework for experimentation to the extent it stops short of specifying how key privacy policies and practices can best be implemented, and to the extent it recommends that utilities and third parties develop forums for sharing information about solutions to common privacy-related problems as Smart Grid-related experience grows. The NIST process for coordinating the development of any privacy standards should remain open and transparent to help utilities plan their Smart Grid investments. EEI encourages the Department to consider any standards-related recommendations offered by NIST.

Dedicated incentives for utility and third party privacy practices and data access policies are not necessary and may be counterproductive. The reward for successful innovation will be continued consumer confidence and satisfaction, which will be a prerequisite for the success of utilities and third party providers alike.

9. Mechanisms to Empower Consumers to Make a Range of Reasonable Choices When Balancing Potential Benefits and Detriments of Privacy and Access

In Question 9, DOE states that 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. DOE asks 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?

The principle that consumers should control who is permitted to access their energy information, with the exception of utilities that require access to such information to provide service, translates into the right of consumers to decide on an individual and case-by-case basis which parties, if any, may receive their data. This is similar to the process in the FCC's rules regarding use of, and access to, CPNI.[14] Notably, the FCC rules outline a customer opt-in/opt-out approval process for telephone company and internet providers offering certain services, customer opt-in approval process for third party access, as well as procedures for obtaining permission to access CPNI. The FCC further mandates specific notice requirements prior to certain uses of CPNI. These rules and procedures offer useful mechanisms enabling customers to make reasonable and informed choices about access to, and use of CPNI and may assist the states and others in developing mechanisms for access to and disclosure of Smart Grid consumers' CEUD.

As discussed above, different consumers will likely desire different degrees of CEUD access, and disclosure and mechanisms must account for these preferences. Some may permit access by multiple parties to broad portions of their data, including HAN data, while other customers may prefer to be more restrictive in granting data access. Similarly, some states and their consumers may wish to allow third parties to transmit data from the utility meter to other devices, while other states and their consumers will not prefer this activity. To provide adequate safeguards empowering consumers, and to

[14] *See* 47 C.F.R. § 64.2007, *et seq*.

account for different degrees of data access, an "opt-in" approval process for information sharing with third parties is the most effective approach for protecting customer privacy interests.[15] It is important to note that once data leaves a utility's meter en route elsewhere than to the utility, it is not easily discernable whether the utility or state regulatory commission will be able to control how that data is subsequently used. Jurisdiction over data in such instances will vary on a state-by-state basis.

Smart Grid and Smart Grid services and technologies are evolving, and it remains uncertain exactly what types of services will be available to consumers. Different types of Smart Grid technologies will demand different mechanisms to empower customers to make reasonable privacy choices. For instance, as the HAN market develops, either a utility-offered HAN solution, or a solution offered through the open market, may develop. Mechanisms empowering customers would vary greatly based on how and where HAN markets develop. Therefore, it would be premature at this point to decide on specific mechanisms for privacy and data access preferences.

It is clear that consumer privacy is important and requires protection. However, setting rigid requirements as part of a Smart Grid strategy is not in the public interest. It would, however, be useful for the Department to offer guidance that highlights the importance of promoting a "smart consumer" who is informed, empowered and able to use electricity and Smart Grid technologies efficiently. In addition, customers should be provided with certain information to allow for reasoned and intelligent choices about how CEUD is accessed. Notably, customers should be informed of the types of customer information that will be collected, from what devices and for what specific purposes; the

[15] This approach is consistent with approval requirements established by the FCC for use of CPNI. *See* 47 C.F.R. § 64.2007(b).

frequency with which the utility will take smart meter readings; and the retention period for all information collected and for what purposes.

10. Security Architecture Provisions for Smart Grid Technologies

In Question 10, DOE asks what security architecture provisions should be built into Smart Grid technologies to protect consumer privacy?

Security architecture requirements to protect consumer privacies depend on particular Smart Grid technologies being implemented. Therefore, it is difficult to predict with any specificity security architecture provisions that should be built into Smart Grid technologies. Nonetheless, there are certain elements of security that should be evaluated for incorporation in the overall of Smart Grid architecture to ensure that customer data is accessible only to authorized parties, maintains its data integrity, and is accessible and available when needed, subject to technological capabilities or limitations in the Smart Grid and components. Security architecture elements to consider for any layer, as technically feasible, may include:

1. Encryption of data in transit when using wireless or non-private wired networks for transmitting sensitive information;
2. Physical segmentation or one-way-only connection from the utility meter and the HAN;
3. Access controls;
4. Authentication of devices participating in HANs and Nationwide Area Networks ("NANs");
5. Authentication of users;
6. Security patches and antivirus processes;
7. Intrusion detection and prevention;
8. Logging and alerting;

9. Physical security at the device level.

NIST is in the process of developing recommended security requirements to protect access to, and communications across, Smart Grid architecture and interfaces.[16] NIST is also examining cyber security risk management strategies in NISTIR 7628, including authentication and authorization of Smart Grid devices and users.[17] The NIST effort to coordinate the interoperability standards development process encompasses numerous stakeholders, including electric utilities, and EEI urges the Department to closely consider NIST recommendations on these and related issues. EEI supports the NIST effort to coordinate the interoperability standards development process, and believes that standards promulgated must facilitate, rather than impede, development of the Smart Grid.

Finally, the Department is well positioned to provide information and direction on security architecture. DOE laboratories have done considerable work on technology modeling, and the industry would benefit considerably by having access to these resources. The Department could further work with manufacturers to develop proof of concepts. Integration testing and equipment certification at independent laboratories would be useful in moving forward with security architecture, as would NIST certifications.

[16] *See* NISTIR 7628, Chapter 2 ("Logical Architecture And Interfaces Of The Smart Grid"); Chapter 3 ("High Level Security Requirements") (February 2010).

[17] *See id*., Chapter 1 ("Cyber Security Strategy"); Chapter 6 ("Research And Development Themes For Cyber Security In The Smart Grid") (subsections 6.4 and 6.6 address security and survivability architecture of the Smart Grid, and other Smart Grid security issues, respectively); Appendix D ("Bottom-Up Security Analysis Of The Smart Grid") (February 2010).

11. DOE Implementation of Smart Grid Mission and Duties While Respecting Jurisdiction and Expertise of Other Federal Entities, States and Localities

In Question 11, DOE asks how it can best implement its mission and duties in the Smart Grid while respecting the jurisdiction and expertise of other Federal entities, states and localities.

EEI recommends first and foremost that the Department support standards development for privacy and Smart Grid interoperability. However, this must be done in accordance with state regulations and rate structures to ensure that regulated utilities can meet obligations to provide safe and adequate service at just and reasonable rates to consumers.

The Department is best suited to provide national leadership on Smart Grid issues such as communications, technical standards, and broad public education about the uses and benefits of the Smart Grid. The Department can similarly serve as a clearinghouse for Smart Grid, by providing guidance, sponsoring forums and funding research. DOE should recognize, however, that many of the actual decisions related to Smart Grid will need to be made by state regulatory bodies, the Federal Energy Regulatory Commission ("FERC") or the FTC, where the jurisdiction and much of the relevant expertise resides. Specifically, as discussed in detail above, issues such as billing determinations, customer information disclosures, marketing and general utilities practices should be addressed at the state level where regulators have a unique awareness of the issues, concerns and expectations of utility ratepayers within a specific jurisdiction.

The Department can nonetheless implement its Smart Grid mission by working with FERC, FTC and the National Association of Regulatory Utility Commissioners ("NARUC") to develop a forum for Smart Grid providers to share information and solutions to common problems. The Smart Grid is composed of new and evolving technologies. Therefore, anticipating and resolving privacy issues and solutions at the outset of deployment is an exceedingly difficult task. The premature adoption of fixed, restrictive standards may likely impair the development of the Smart Grid. It will, however, be useful for Smart Grid participants to have institutional mechanisms for the exchange of information as Smart Grid implementation grows. It would be helpful for all stakeholders for the Department continue its support of Smart Grid research, as well as support for the NIST effort to coordinate the interoperability standards development process.

12. Access to Energy Consumption Data By Authorized Federal, State or Local Government Agents

In Question 12, DOE asks when, and through what mechanisms, should authorized agents of Federal, State or local governments gain access to energy consumption data?

Utilities have a long track record of cooperating with law enforcement agencies while at the same time protecting consumer privacy. Utilities have long-standing procedures dictating how they handle such requests for information. Traditionally, law enforcement agencies have been granted access to CEUD pursuant to appropriate legal processes. To the extent certain information disclosure is required by law, utilities will continue their current practice of cooperating with government authorities making legally

compliant government information requests by providing information requested in compliance with applicable state and federal laws.

If a non-law enforcement type governmental agency desires CEUD or other energy use information (*i.e.*, for determining levels of compliance with certain government-authorized energy programs such as demand-side management plans), in most jurisdictions, agencies are required to submit such requests through a filing with the appropriate state regulatory authority, which would deliberate and issue a written order determining whether to require a jurisdictional utility to release aggregate usage data to that agency and whether such information should be subject to a protective order or confidentiality requirements to ensure protections of customer privacy. This practice will ensure that proper relationships are maintained between jurisdictional utilities, state regulatory authorities, and non-law enforcement governmental agencies.

Further, utilities will continue to provide all information related to products and services in the event of a theft of energy or services, or provide disclosures as necessary for protection of public health, safety or welfare. Third party service providers should adhere to similar standards.

13. Third Party Access to Energy Information: Who Should Have Access; How Should Access be Gained; What Standards Would Assist Third Parties in Protecting Energy Information

In Question 13, DOE asks 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?

The ability of authorized third parties to obtain energy usage data must be clarified. While authorized third parties should have access to energy usage information, customer authorization and third party compliance with data access standards are necessary to ensure customer privacies. Both types of energy consumption data – CEUD (customer-specific data) and operational data (aggregated, non-customer specific data) – require unique protections. The mechanisms for the delivery of CEUD to third parties may involve costs that should not be borne by utilities. Operational data (aggregated, non-customer specific data) which is proprietary utility information should not be accessible to third parties without utility consent.

A. CEUD

The need for protecting retail consumer and utility privacies must always be carefully balanced with the need for promoting innovation of technology. Utilities should not be required or permitted make CEUD accessible to authorized third parties without affirmative and informed authorization from the affected customer. Exceptions to this general rule are where release of data is required under applicable law (*i.e.*, provision of data to law enforcement agencies or the relevant state regulatory authority), or in instances of reliability emergencies, when utilities should be permitted to provide CEUD to energy system operators if needed to maintain safety and reliability. Any authorization and release of customer data to third parties, however, must be done in a manner consistent with all applicable laws.

To protect access to CEUD and to prevent fraud, third parties must follow all principles and business practices recommended for utilities, prior to being eligible to receive CEUD. Third parties should also be required to obtain explicit authorization

from a utility customer prior to gaining access to that customer's CEUD. Further, third parties authorized to receive CEUD should be subject to disclosure requirements, and should be required to share with utilities data protection responsibilities. They should also be liable for all liabilities resulting from any unauthorized access to CEUD. Authorized third parties must also be required to obtain affirmative and informed consent from customers prior to reselling or disseminating CEUD. To ensure that customer consent fully contemplates the scope of CEUD they are consenting to disclose, customers must be provided with clear information on, among other things, the nature and use of this data. Absent such information, the significance of a consumer's consent to disclose CEUD is uncertain.

As detailed above, privacy regulation of customer data has traditionally been the responsibility of the states, which have developed various privacy protection laws for customer data. Virtually all electric utilities have their own data ownership policies in accordance with regulations promulgated by state regulatory authorities. As Smart Grid technologies and applications develop, treatment of information generated from smart meters, HANs and devices connected directly for third party access will require third party standards for handling and protecting this data. The NISTIR 7628 provides a thoughtful evaluation of the privacy exposures that may be created in Smart Grid environments, and helps to identify appropriate practices for meeting these new exposures.[18] EEI recommends that the Department likewise view this NIST effort as a thoughtful approach to standards, guidelines, and practices for third parties in handling and protecting CEUD.

[18] The results of this NIST effort will be documented in Chapter 3 ("Privacy and the Smart Grid") of NISTIR 7628.

Further, the FCC has established extensive safeguards on disclosure of CPNI, as well as standards and procedures for third party verification.[19] EEI recommends that DOE consider these procedures, among others, for third party verification and related liabilities for unauthorized disclosure of CEUD.

In many instances, securing customer consent electronically may be more expedient and cost-effective than a "wet signature." All other customer education information, including an explanation of the details of possible information which could be provided after customer authorization, could be explained on the form itself, as well as on the website. Customers should also be given the option to consent via paper form.

All data shared by utilities with third parties should be done through accepted and secure methods of data transportation, using reasonable methods that are technically feasible for the utility. Third parties must comply with standard methods and formats used by utilities to transfer meter usage data, to minimize expenses involved with system integration for different methods of data transfer. Further, third party vendor products and services should comply with applicable state and state-approved utility requirements and any NIST interoperability standards prior to gaining access to CEUD.

B. Operational Data

Once CEUD is aggregated it is no longer customer-specific. To protect against improper disclosure of customer-specific information, utilities should make certain that no personal information, including customer identifiers (*i.e.*, service address, billing address, account number), is included in aggregated data.

[19] *See* 47 C.F.R. §§ 64.1120-40, 64.2010.

Third parties do not have any rights to access validated CEUD, except as properly authorized by the consumer. Likewise, third parties do not have any rights to aggregated customer usage data. Nor should third parties have such rights given that, in the case of verified data, such information is proprietary in nature. Utilities often enhance CEUD, using software programs to validate, estimate and edit raw metered data, or using decision support systems consisting of a data base, model base, and user interface. To the extent utilities enhance CEUD, neither customers nor third parties have a right to access such enhancements. These types of data are enhanced and validated by utilities for internal purposes, and utilities therefore have specific ownership rights to this data that prevent its disclosure to customers or third parties.

Releasing aggregated usage data may implicate cyber security concerns, as this information contains detailed locational energy consumption information that is used for bulk power system reliability purposes, to ensure a utility can adequately meet daily and seasonal peak loads. Allowing or mandating access to this information would result in an increased number of power system entry points and paths for potential adversaries to exploit. This in turn could result in system vulnerabilities, which might allow unauthorized parties to alter load conditions to destabilize the grid in unpredictable ways.

14. Forms of Energy Information Accessible to Consumers or Third Parties

In Question 14, DOE asks what forms of energy information should consumers or third parties have access to?

Utilities provide consumers on every electricity bill CEUD that has been collected, verified and authenticated by the utility. Consumers should have access to

usage information that their utility or metering authority collects (*i.e.*, kW, kWH, kVAR, etc.), and in the same validated (*i.e.*, billing-quality) form that the utility uses it. While direct consumer access to CEUD does have some potential advantages, smart meters introduce significant concerns about the provision of raw, unaudited data directly to consumers or third parties from the meter. State regulatory authorities should carefully weigh the benefits of this practice. Use of raw data could create billing confusion as consumers try to estimate their own bills, which in turn could undercut consumer confidence and expectations regarding accuracies of their usage data. Similarly, depending upon the manner in which raw data is made available to the consumer or third party, the provision of this data could create additional privacy and security issues.

Third parties should only have access to data a customer consents to share through an agreement, or through enrollment in an energy efficiency program, subject to any technological capabilities or limitations in the utility smart meter/advanced metering infrastructure ("AMI") system. Third parties should only have access to the same type of energy information as entitled to by utility customers. Such energy information should only be available to authorized third parties, and through accepted and secure methods of data transportation, using reasonable methods that are technically feasible for the utility.

As discussed above, utilities often enhance CEUD, using software programs to validate, estimate and edit raw metered data, or using decision support systems consisting of a data base, model base, and user interface. To the extent utilities enhance CEUD, neither customers nor third parties should have a right to access such enhancements except to the extent such modified, enhanced or augmented data is provided in customer billing statement. Similarly, as discussed above, neither customers nor third parties (with

the exception of affiliates or other entities presently relied upon by utilities internally) shall have access to aggregated energy usage data.

15. Consumer Access to Personal Energy Information in Real-Time or Near Real-Time

In Question 15, DOE asks what types of personal energy information should consumers have access to in real-time or near real-time?

EEI believes consumers should have access to energy price information; particularly, if dynamic pricing has been implemented in their service territory. Time-differentiated price signals (*e.g.*, critical peak prices, peak time rebates) are essential to motivate demand response. Customers need to see when prices are high so they can avoid costs by curtailing usage. However, prices do not need to be provided in real-time; day-ahead forecasts serve the purpose very well. Of course, customers (or their devices) do need to see system emergency (*i.e.*, critical peak) signals in real time.

Regarding energy consumption data (*i.e.*, kWh usage data in 15-60 minute intervals), EEI believes that calls for access to such data in real, or close to real time do not take account of the costs involved, or the limited benefit to consumers. The cost can be substantial. If interval data is ported from the utility meter to displays and/or data management systems on the customer side of the meter, the cost may be on the order of $100-$200 per customer, or several hundred million dollars for a large utility. If raw interval data is taken back to the utility, processed so it is accurate enough to render customer bills, and stored in a meter data management system so it can be searched and retrieved by customers in close to real time, the cost can be billions of incremental dollars

per utility, and can require substantial replacement of utility infrastructure, including infrastructure currently being built as part of Smart Grid deployments.

EEI believes it is telling that it is not customers who are asking for real-time data; it is third parties, presuming to speak for customers. Third parties want the data for their own business purposes, and wish to pass these added costs on to consumers through utility bills, thereby having consumers subsidize their commercial activities. Consumers, for their part, have little interest in real-time data, and are generally indifferent to electricity price changes. Indeed, it is a continuing challenge for the industry and policymakers to educate consumers on the benefits of demand response and increased energy efficiency. Even then, consumers will not have a need for real-time or near real-time consumption data. Consumers may be interested in their bill-to-date in the current billing cycle; their energy usage in relation to personal goals or average consumer consumption; or receiving time-differentiated price signals so their home area networks can dispatch appliances (*e.g.*, "prices to devices"). None of these uses or functions requires real-time or near real-time consumption data.

The bottom line is cost and cost allocation. Regulated utilities conduct cost/benefit analyses to decide whether and how to deploy Smart Grids. To the extent policy makers mandate costly access to near real-time data, they should consider the direct beneficiaries of such access in determining who should pay for it.

16. State Efforts to Implement Policies for Smart Grid Privacy, Data Collection and Third Party Use of Information

In Question 16, DOE asks what steps have states taken to implement Smart Grid privacy, data collection, and third party use of information policies?

States have been very active in implementing consumer protections against unfair and deceptive practices, and privacy protections of customer data. Further, many states have "anti-hacking" statutes prohibiting gaining unauthorized access to computers (including smart meters).

In addition, security breach notification laws are state-level statutes that generally require any person or organization that controls personally identifiable information to report instances of unauthorized access. Presently, 45 states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted security breach notification laws.[20]

17. Efforts of Investor-Owned Utilities, Municipalities, Public Power Entities and Electric Cooperatives to Implement Policies for Smart Grid Privacy, Data Collection and Third Party Use of Information

In Question 17, DOE asks 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?

Electric utilities all have privacy policies in place that pre-date Smart Grid development. Further, as noted earlier, utilities have a strong track record of protecting the privacies and energy usage information of their customers. EEI's members recognize the importance and need of reviewing and possibly updating policies and practices necessary to address new privacy issues raised by the development of "smart technologies" in connection with the Smart Grid. To this end, EEI's members are developing consensus guidelines to provide a framework for reviewing and updating privacy and data access policies.

[20] *See* Nat'l Conf. of State Legislatures, State Security Breach Notification Laws (Dec. 9, 2009), *at* http://www.ncsl.org/default.aspx?tabid=13489 (providing links to statutes).

In addition, EEI members have taken a number of steps individually to address privacy concerns arising from Smart Grid, and to develop, review and update internal privacy policies. Such efforts include creation by some EEI members of a "Privacy Officer" position, charged with overseeing corporate privacy policy issues, as well as monitoring for necessary policy changes, and responding to privacy-related concerns and inquiries. Likewise, other EEI members are tasking existing compliance officers with similar responsibilities. The need for a new Privacy Officer position, as recognized by some utilities, arises from privacy issues greater than those posed exclusively by Smart Grid development.

Some EEI members are forming internal organizations to review customer privacy issues and policies. Utilities are also gathering input and expertise from their legal departments in review of state privacy requirements as applied to customer privacy. Other utilities have developed data access policies to be implemented prospectively, based on the privacy and data access consensus guidelines developed by EEI's members.

One particular program initiated by Consolidated Edison Company of New York, Inc. (“ConEdison”) includes a HAN demonstration project involving approximately 300 customers who will have one of three different types of HAN technologies and approximately 1200 customers who will have a web service application to display their meter usage. The HAN technologies are represented by three different vendors and variations of hardware combinations. As part of this pilot program, ConEdison is reviewing security measures each HAN provide is implementing to protect the privacy of the energy usage information. One key security requirement for these programs is SAS70 certification. ConEdison also has administrative controls in place with vendors

including non-disclosure agreements and contractual language that requires them to keep customer usage information private. ConEdison is sharing meter usage information through secure file transfer protocol ("FTP") from its corporate network to vendors' secure databases

18. Consideration of Consumer Data Accessibility Policies When Evaluating Future Smart Grid Grant Applications

In Question 18, DOE asks whether it should consider consumer data accessibility policies when evaluating future Smart Grid grant applications?

The Department should not consider consumer data accessibility policies when evaluating grant applications for Smart Grid technologies, as doing so would be premature at this point given that Smart Grid technologies are still evolving. Further, state policies addressing information accessibility policies are already in place. The Department should defer to states on these matters. It is important that Smart Grid grants be focused on demonstrating new Smart Grid technologies. Consideration of data access policies as part of this demonstration process would result in needless delays in the evaluation of Smart Grid grant applications, and would cause considerable delays in development of Smart Grid technology.

Further, consumer data accessibility may be an option available to consumers as part of specific third party services (*i.e.*, in Texas, consumer data access is provided where a consumer purchases specific equipment or services). For these reasons, consumer data accessibility should not be a requirement for Smart Grid grant applications or for implementation of Smart Grid technologies.

CONCLUSION

EEI respectfully requests that the Department consider these comments and ensure that any DOE recommendations regarding Smart Grid data access, third party use and privacy is consistent with them.

If the Department has any questions about these comments, please contact Eric Ackerman, Director Alternative Regulation, at eackerman@eei.org or 202-508-5528, or Greg Obenchain, Manager of Distribution Operations and Standards, at gobenchain@eei.org or 202-508-5138.

Respectfully submitted,

EDISON ELECTRIC INSTITUTE

/s/ David K. Owens
David K. Owens
Executive Vice President

Aryeh B. Fishman
Director, Regulatory Legal Affairs
Office of the General Counsel

Edison Electric Institute
701 Pennsylvania Avenue, NW
Washington, DC 20004-2696
(202) 508-5000
afishman@eei.org

H. Russell Frisby, Jr.
Jonathan P. Trotta
Counsel
STINSON MORRISON HECKER LLP
1150 18th Street, NW, Suite 800
Washington, D.C. 20036-3816
(202) 785-9100
(202) 785-9163 (Fax)
rfrisby@stinson.com
jtrotta@stinson.com

Dated: July 12, 2010