

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



August 9, 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 reply 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

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"); *see also* Notice

As detailed in EEI's initial comments,² EEI supports 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 provide safe and reliable electric service.

INTRODUCTION

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 raises new and significant privacy and data access issues, requiring electric utilities to consider possible updates to their policies and procedures. EEI's members are committed to protecting customer privacy, and are working diligently to ensure that our policies and procedures address new and emerging access and privacy issues.

Commenters in this proceeding highlight the numerous consumer benefits that will result from deployment of Smart Grid technologies and services, and offer examples of cutting-edge functionalities that may allow consumers to control and monitor energy usage and appliances. Some of these technologies have already been implemented as utility pilot programs in various jurisdictions. Nonetheless, EEI cautions the Department

of Extension of Public Comment Period for Reply Comments, 75 Fed. Reg. 42,727 (2010) (extending comment date from July 26, 2010 to August 9, 2010).

² See Comments of the Edison Electric Institute, DOE NBP RFI: Data Access (filed July 12, 2010) ("Initial Comments").

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).

and state and federal regulators not to lose sight of the underlying Smart Grid issues in need of deliberation: data access, privacy and costs.⁴

As the Smart Grid evolves, strong data access and privacy policies are needed to protect against unauthorized access and use of CEUD in the possession of utilities. Third parties⁵ face strong incentives to capitalize on the value of CEUD, which may be inconsistent with the interests of utility customers and the efforts of utilities and states to protect that information against unauthorized disclosure at the utility level. 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 should be responsible for protecting this information. While utilities can and will take proactive steps to implement policies and procedures safeguarding CEUD while in their possession, customers must become educated on the new privacy exposures presented by access to this data by third parties.

Careful consideration must be given to the types of energy information consumers or third parties have access to, as well as the intervals at which this information is to be made available. Costs associated with providing access to energy consumption data in real, or close-to-real time can be substantial and far outweigh any perceived benefit to consumers. To the extent policy makers mandate costly access to real or near real-time data, ample consideration should be given to the identity of the beneficiaries of such access in determining who should pay for it. These significant cost and cost allocation

⁴ EEI also directs attention to the need for dedicated spectrum to support all of these goals in response to the DOE's RFI. *See* comments of the Edison Electric Institute, DOE NBP RFI: Communications Requirements, at 24-28 (filed July 12, 2010).

⁵ "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.

issues cannot be overlooked as utilities, as regulated entities, must conduct cost/benefit analyses to decide whether and how to deploy Smart Grids.

In addition to these and other points raised in our Initial Comments, EEI respectfully requests that the DOE consider the following:

REPLY COMMENTS

A. Energy Consumption Data Ownership

In its Initial Comments, EEI explained that data ownership is traditionally governed by state law and varies on a state-by-state basis. 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.

Several commenters generally assert that energy usage data is owned exclusively by the consumer. According to Elster, consumers typically own this data under state law. Honeywell argues that "detailed consumption data" reflects consumers' private lives and should be owned and controlled solely by the consumer. CPower, Inc. ("CPower") contends that "individual consumption data" is owned by the individual, while others "may in some cases have a right to use that data." The Building Owners and Managers Association ("BOMA") believes that property owners, or in some instances tenants, own this data and, therefore, that "utilities must be compelled to provide" whole-building aggregate monthly energy consumption data, free of charge, to building owners and managers upon request.⁶ In the view of several demand-side management groups, all or

⁶ BOMA Initial Comments at 2, 3.

certain types of data is "co-owned" between, among others, utilities, consumers, grid operators and transmission owners, and jurisdictional governmental entities.

As evinced in these responses, the issue of data ownership is varied based on interest. While many commenters posit interesting theories on energy consumption data ownership, the fact remains that ownership of this data varies by jurisdiction and is governed by individual state laws. Ownership of energy usage information cannot simply be asserted, but must arise from an established legal basis. It should be acknowledged that a strong case can be made for utility ownership of CEUD. However states will need to determine these issues, and retail access states may have already adopted laws addressing data ownership and usage. For example, under Texas law while consumers served by investor-owned utilities own their energy consumption data, utilities still have certain protected rights to use this data for business and operational purposes.⁷ EEI reaffirms that an approach to Smart Grid data access based on property rights and ownership interests in energy usage data is problematic and will complicate efforts to develop a framework for Smart Grid data access policies.

Instead, as pointed out by EEI, the National Rural Electric Cooperative Association ("NRECA") and others, the critical policy issue for Smart Grid development is not ownership of consumption data, but access to, usage and disclosure of that data. The role of the states in developing data access and privacy standards cannot be overlooked, as states have jurisdiction over the relationship between the utility and the retail customer out of which this data arises. Privacy regulation of customer data has traditionally been the responsibility of the states, which have developed various privacy

⁷ See Oncor Electric Delivery Company LLC Initial Comments at 2.

protection laws for customer data. States also have consumer protection laws safeguarding interests of energy consumers.

Even if, as commenters suggest, customers were to own their usage data, utilities must continue to have full access to and control over all CEUD, including operational data⁸ and granular data, as part of their legally-mandated obligation to provide safe, reliable and cost-effective service. This information is required for reliability purposes, to ensure utilities can adequately meet daily and seasonal peak loads, and to make certain that utilities are continually aware of new system loads as well as existing and future penetration. EEI reaffirms that 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.

B. Privacy Protections and Practices

In its Initial Comments, EEI explained that 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. As stated in EEI's Initial Comments, it must be clarified that commercial and industrial end-use customers (in addition to residential customers) also

⁸ "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.

require privacy protections so as to avoid potential competitive harm that might arise from the unauthorized dissemination of their energy consumption and cost information.

Similarly, utilities, as businesses, are legally entitled to certain privacy protections which extend to, among other things, proprietary and validated CEUD, aggregated non-customer specific energy usage data, as well as technical functions associated with meters and supporting communication infrastructure. The need for protecting consumer and utility privacies must be carefully balanced with the need for promoting cost-effective innovation of technology.

In the context of privacy, the United States Telecom Association ("USTelecom") asserts that the Smart Grid initiative "represents a clean slate from which to work." Such a broad assertion is troubling on many levels. Notably, consumer privacies related to energy usage information are already protected under state laws and state-mandated practices for utilities. To this end, privacy structures have been in place at the state level for some time. In addition, 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.

Several commenters offer specific recommendations on privacy practices that should be considered and implemented to protect energy information. These recommendations range from use and collection limitations to data quality rules. As EEI stated in its Initial Comments, however, Smart Grid technology is new and evolving, and it is premature to decide what privacy practices should be implemented to protect

consumer information.⁹ EEI agrees with the Consumer Electronics Association ("CEA") that existing privacy best practices and policies exist and can be used to support this nascent industry. However EEI adds that privacy practices must be sufficiently transparent for customers, utilities and third parties, and must facilitate, rather than impede, Smart Grid development. Utilities have a strong track record of safeguarding the privacies and energy usage information of their customers based on existing practices and regulatory structures. There is no reason for the DOE to attempt to establish specific standards to protect energy information in light of standards currently being developed at all levels of state and federal government and in a myriad of Congressionally-sanctioned organizations (*i.e.* NIST, FERC, and the states). EEI encourages the Department and state regulatory authorities to consider the National Institute of Standards and Technologies' ("NIST") guidance and recommendations on data issues so as to avoid developing definitions or standards that might be inconsistent with existing data treatment practices.¹⁰

Honeywell comments that any form of centralized storage of consumption data, or use of networks to move data, presents unnecessary privacy and security risks, adding that privacy and security are best served by transmitting detailed data directly from the meter into the customer premises. EEI notes, however, that privacy and security of energy usage data are two very different issues. Utility networks and storage facilities offer considerable security protections for the transmission of usage data, and any

⁹ Different retail utility customers will have different privacy needs, and 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.

¹⁰ See NIST report *Smart Grid Cyber Security Strategy and Requirements* ("NISTIR 7628") (February 2010).

development of infrastructure as part of the Smart Grid would ensure similar security protections. At issue here are privacy protections of this usage information and, as stated herein and in EEI's Initial Comments, utilities act responsibly with data storage and access.

EEI reaffirms its belief that state regulatory agencies should consider developing consistent procedures for third parties verifications, and urges the states to consider the FCC's rules addressing these issues.¹¹

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

In its Initial Comments EEI clarified that, for practical reasons, utilities must have control over their deployment of their infrastructure. EEI explained that allowing consumers to opt out of meter deployment would result in adverse financial and operational impacts that would be felt by all retail electric customers. Notably, the ability to opt out of meter deployment would create "data holes," and hinder electric utility efficiency in deploying smart meters and utilizing Smart Grid technology, in turn raising costs. Service reliability would also be adversely impacted. For these reasons, meter deployments have always been managed between utilities and state regulators.

EEI shares the view of the majority of commenters in this proceeding that saturation deployment of smart meters is necessary to maintain reliable service, to achieve certain efficiencies and to reduce consumer costs. As EnerNOC notes,

¹¹ See, e.g., 47 C.F.R. § 64.2009 (safeguards for use of customer-specific information including); see also 47 C.F.R. § 64.2010 (safeguards against unauthorized disclosure of CPNI); see also 47 C.F.R. § 64.2011 (procedures for notifying law enforcement).

"[c]onsumers 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 large grid operation and maintenance purposes such as service initiation and outage detection."¹² NRECA points out that utilities are deploying smart meters for a variety of beneficial uses beyond just enhancing information that can be presented to the consumer, and adds that the realization of these benefits by all of the utility's customers would be significantly undermined if some consumers declined to have a smart meter installed. NRECA correctly notes that allowing consumers to opt out of smart meter deployment would introduce unnecessary burdens and costs in an already challenging process, and would undermine the business case for investment in smart meter technology.¹³

EEI disagrees with the National Consumer Law Center, *et al.* ("NCLC"), that smart meter installation, especially for low-volume users, should be voluntary. According to NCLC, if "smart meters are not cost-effective for the particular sector of the population, but the utility wants to install meters, then these populations should not have to foot the bill for benefits they will not receive."¹⁴ Allowing "sectors" of utility consumers to opt out of deployment would considerably undermine the ability of utilities to efficiently roll out smart meters, and would increase costs to all ratepayers. In addition, certain benefits of smart meters would be rendered ineffective if large segments of the population were permitted to opt out. Service reliability would likewise be impacted.

¹² EnerNOC Initial Comments at 3.

¹³ NRECA Initial Comments at 12-13.

¹⁴ NCLC Initial Comments at 5.

EEI further takes issue with NCLC's presumption that certain customers would be made to pay for benefits not received. As EEI highlighted in its Initial Comments, saturation deployment of smart meters is a "win-win" scenario for customers who will receive the benefits from network modernization afforded by deployment of Smart Grid technology (*i.e.*, improved power quality, increased reliability, increased safety, faster service restoration, increased utility productivity). While utilities must have control over deployment of their smart meter infrastructure or hardware, these issues should be addressed at the state level.

Finally, EEI supports the National Association of State Utility Consumer Advocates' ("NASUCA") position that questions of whether or when to install smart meters, and under what conditions, should be addressed at the state level. EEI notes that meter deployment decisions, including the deployment of smart meters, are addressed by state regulatory commissions. To the extent states make smart meter deployment determinations, all deployment issues related to those meters should also be addressed exclusively by the appropriate state regulatory commission.

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

In its Initial Comments, EEI emphasized that electric utility data policies and practices are applicable to all communities and customer classes, and protect all consumers equally, and that 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. All consumers, including low-income consumers, will

benefit from the optimized management of electricity demand and from increased reliability and capacity of the grid resulting from the Smart Grid. These benefits 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, or customer access to, Smart Grid technologies.

Several commenters detail specific procedures and policies that should be implemented under the auspices of protecting low-income customers. According to NASUCA, policies and programs should be implemented to prevent the inequitable distribution of Smart Grid benefits among customers, and to ensure that customers participating in low-income programs will be no worse off under the Smart Grid. The Joint Center for Political and Economic Studies ("JCPES") advocates for numerous protections, including making Smart Grid devices more affordable. According to JCPES, many unknown vulnerabilities exist for low-income consumers under advanced metering initiatives, such as increase pricing that could impact the well-being of low-income customers and senior citizens.

EEI notes, however, that these and other issues affecting vulnerable classes of customers are traditionally examined and addressed in proceedings before state utility commissions. Even Tendril notes that "[s]tate agencies and regulatory bodies have long experience addressing the needs of these communities that can serve as models moving forward."¹⁵ The issues raised by NASUCA, JCPES and others are among those that are closely considered by state commissions as they develop meter deployment and pricing plans and programs benefitting low-income customers. Smart Grid initiatives and

¹⁵ Tendril Initial Comments at 5.

deployments will be treated similarly before state commissions. As Tendril adds, some states have already established target programs intended to accompany smart meter deployment, citing a Texas program created to distribute in-home energy monitors to low-income consumers served by smart meters.

EEI agrees with JCPES to the extent that electric utilities believe that Smart Grid infrastructure expenditures should be made in densely populated urban and low-income areas as well as throughout the rest of utility service areas. As explained above, and in EEI's Initial Comments, failure to uniformly deploy Smart Grid infrastructure, or to allow consumers to opt out of meter deployment, would result in adverse financial and operational impacts. It would create "data holes," thus hindering electric utility efficiency in deploying smart meters and utilizing Smart Grid technology, and raising costs to all consumers. In this instance, the issue does not pertain to untimely broadband deployment of the type which was recently addressed by the FCC.¹⁶ Instead, the point is that network efficiency requires that Smart Grid technology must be deployed to densely populated and low-income areas. Similarly, limiting Smart Grid investments to densely populated areas only could result in similar inefficiencies and might not achieve the full value of the technology. Because Smart Grid enables remote meter readings, this is especially important for eliminating service truck trips in low-density areas of a utility's territory. This translates into operational cost savings for the utility and its ratepayers. The benefits of Smart Grid are for all consumers, and limiting the deployment of Smart Grid technologies in this manner would undoubtedly hamper utility investment in, and customer access to, Smart Grid technologies. Service reliability enhancements

¹⁶ See Sixth Broadband Deployment Report at 19 FCC Dockets GN 09-137 and 09-51 (Released July 20, 2010).

attributable to Smart Grid investments should not be unreasonably limited to designated portions of the utility's grid, particularly in cases of mass deployment.

Nonetheless, EEI agrees with NASUCA and others on the need for Smart Grid education. Utilities recognize that customers must become 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, printed materials are available that provide customers 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. Customers can also contact their utility's customer service to obtain this information.

E. Security Architecture Provisions for Smart Grid Technologies

In its Initial Comments, EEI stated that 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. EEI went on to highlight 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.

EEI agrees with NRECA that developing a security architecture in tandem with designing the Smart Grid system itself and accompanying engineering processes is a significant challenge.

Several commenters offer specific security architecture features for incorporation into Smart Grid technologies. Honeywell identifies meter firewalls, on-premises media access within the home area network ("HAN") and an internet gateway as architecture features. According to NASUCA, open standard protocols for security architecture should be developed. NASUCA adds that security architecture features should include embedded cyber security, encryption, physical and operational safeguards, and support multi-point to multi-point communications. Silver Spring Networks states that robust cryptography based on publicly-developed and field-hardened standards should be required. EnerNOC and the Demand Response and Smart Grid Coalition ("DRSG") state that Smart Grid technologies can borrow security architectures from other areas of commerce (*e.g.*, online banking and shopping).

While commenters offer useful information, EEI reaffirms its opposition to adopting specific security requirements at this time due to the relatively nascent field of Smart Grid technologies. EEI does support the inclusion of basic security features now, such as those mentioned in EEI's Initial Comments, into new Smart Grid technologies.¹⁷ However, because Smart Grid technologies may not meet standards that have yet to be

¹⁷ See EEI Initial Comments at 25-26 (listing certain "[s]ecurity architecture elements to consider for any layer, as technically feasible. . .").

developed, and to avoid discouraging investment or imposing an under- or over-inclusive "one-size-fits-all" architecture, EEI cautions against the retroactive application to technologies of specific security features that were not available when those technologies were deployed. As specific security features are adopted, they should be built into all new Smart Grid technologies, and not added on later by utilities.

EEI supports the comments of Tendril, DRSG and other demand side management commenters, as well as NRECA, APPA and others to the extent they highlight the standards development work being done in this area by NIST. As stated in EEI's Initial Comments, NIST is in the process of developing recommended security requirements to protect access to, and communications across, Smart Grid architecture and interfaces.¹⁸ NIST is also examining cyber security risk management strategies in NISTIR 7628, including authentication and authorization of Smart Grid devices and users.¹⁹ The NIST 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 standards development process, and believes that standards promulgated must facilitate, rather than impede, development of the Smart Grid. Finally, EEI firmly believes that the Department is well positioned to provide information and direction on security architecture by making resources on technology modeling available to the industry.

¹⁸ See NISTIR 7628, Chapter 2 ("Logical Architecture And Interfaces Of The Smart Grid"); Chapter 3 ("High Level Security Requirements") (February 2010).

¹⁹ 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).

F. 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

EEl stated in its Initial Comments that 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. In all instances, the need for protecting retail consumer and utility confidentiality must always be carefully balanced with the need for promoting innovation of technology.

EEl generally agrees with commenters on issues of third party access to energy information, namely that only customer-authorized third parties should have access to energy usage information. EEl emphasizes, however, that important distinctions between CEUD and operational data require that access to these types of data by third parties be considered and addressed separately. Therefore, EEl's response to third party access comments will be addressed in this manner.

1. CEUD

Utilities should not be required or permitted make CEUD accessible to authorized third parties without affirmative and informed authorization from the affected customer. Exceptions exist where release of data is required under applicable law or in instances of

reliability emergencies. Any authorization and release of customer data to third parties, however, must be done in a manner consistent with all applicable laws.

According to CPower, informed and explicit customer authorization alone should be sufficient for third party access CEUD. Permitting unfettered third party access is insufficient and overlooks important state-based consumer protections, as well as the need for third party verification. EnerNOC suggests that handling and protection of data by third parties should be addressed through direct agreements between consumers and third parties. While contractual arrangements may be a component of the consumer-third party relationship, additional requirements must be implemented to ensure the privacy rights of consumers. 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.

As discussed in EEI's Initial Comments, 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. EEI agrees with EnerNOC that authorized

third parties should only use consumption data for purposes explicitly consented to by the consumer.

According to CEA, consumers should be able to direct utilities to make energy consumption data available to third parties in a consistent, machine-readable format. However, this leaves many questions as to the format and method in which this data should be provided, and places little responsibility on third parties themselves to comply with accepted and standardized formats. EEI previously stated in its Initial Comments that 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.

To the extent CEA suggests development of national interoperability standards and data formats, EEI adds that 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. As Smart Grid technologies and applications develop, treatment of information generated from smart meters, HANs and devices connected directly to meters must comply with utility or governmental rules about what can be connected to a meter. 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.²⁰ 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.

BOMA states that benchmarking of energy consumption and costs require building owners and managers to access whole-building aggregated utility consumption and costs data on a monthly basis for each fuel type used by the building. According to BOMA, utilities should provide this information to building owners and managers without the need for authorization from each tenant as a utility customer of record. BOMA notes that many jurisdictions are starting to mandate benchmarking, and require reporting of certain standard energy metrics.²¹ To the extent jurisdictions consider requiring these practices, it is important to note that aggregating energy usage data and cost information for a single building presents significant practical and costly problems for utilities. Aggregating data for an entire building requires utilities to search for predecessor accounts for each building unit, which demands substantial manual labor and calculations. In addition, providing building owners and managers with tenants' energy usage information raises a number of separate privacy issues itself.

2. Operational Data

Several commenters reveal that *all* energy usage information should be made available to third parties once authorized by consumers. As EEI indicated in its Initial Comments, however, third parties do not have rights to aggregated customer usage data. Once CEUD is aggregated it is no longer customer-specific, as all personal information

²⁰ The results of this NIST effort will be documented in Chapter 3 ("Privacy and the Smart Grid") of NISTIR 7628.

²¹ BOMA Initial Comments at 3.

including customer identifiers (*i.e.*, service address, billing address, account number), is removed. Information contained in aggregated usage data reveals 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. Releasing this information raises significant cyber security concerns and could result in system vulnerabilities, allowing unauthorized parties to destabilize the grid in unpredictable ways.

Further, given its proprietary nature, third parties should not have access to verified data. 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 form of proprietary data that prevent its disclosure to customers or third parties.

Finally, DRSG, UTC and others are correct that third party contractors or service providers working directly with utilities should continue to have access to consumption data, as necessary to carry out utility functions (e.g., billing, etc.). As APPA notes, third party contractor access to data in these instances should extend only to the performance of the contracted service, and utilities should continue their practice of ensuring that these third parties comply with utility confidentiality requirements.

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

In its Initial Comments, EEI stated that 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. Third party access to CEUD (upon customer consent) should be subject to technological capabilities or limitations in the utility smart meter/advanced metering infrastructure (AMI) system. Authorized third parties should only have access to the same type of energy information as entitled to by utility customers, with such information being available through accepted and secure methods of data transportation, using reasonable methods that are technically feasible for the utility.

EEI agrees with NASUCA and NRECA that state regulatory agencies will have an important role in determining types of data that will be available and at what level of granularity. As NRECA points out, states and retail regulators are experienced at weighing these factors and are well positioned to understand the needs and interests of local consumers.²² EEI believes that state commissions should further recognize that the most efficient and cost-effective methods for customer and third party access to information is through established methods relied upon by utilities for data collection.

Several commenters suggest imposing upon utilities new data collection requirements that are significantly more stringent than methods used today. Mandating such requirements will create new and substantial costs. For example, Verizon states that information such as current price, current use rate (e.g., kWh), amperage, current voltage and voltage stability for the last hour/12 hours (e.g., 110 vac +/- .5 volts), outage data, historical price and usage are relevant and should be made available. DRSG and Tendril

²² NRECA Initial Comments at 16.

suggests availability of real-time generation source information and emissions profiles; customer-specific power quality data and relevant wholesale prices, as well as peak-time rebate opportunities, customer specific power quality data and other information. Google states that granularity of data provided to the consumer should be in at least 15-minute increments, adding that providing data on an hourly or less frequent basis is not as useful.²³ However, requiring utilities to comply with providing such detailed and complex data, which is beyond the scope of data normally collected or made available by utilities, will impose significant additional costs associated with comprehensive network upgrades, storage and other infrastructure to manage and transmit this information to the meter. Interestingly, most requests for such detailed information come from demand response providers, and other service and technology providers on the customer side of the meter. Notably, none of these commenters offer any suggestions whatsoever for addressing the considerable costs of providing this information.

EEI believes that, to the extent third parties desire access to more detailed energy usage data, access to data on a more frequent basis, or at a more granular level, the associated costs of providing such information should be borne by those third parties and not the utility customer. Third parties appear to want this data for their own business purposes at the expense of consumers. In contrast, utilities, as regulated entities, are financially accountable under law to states and customers and must be certain that their investments are for the benefit of consumers – not every Smart Grid third party provider.

EEI disagrees with BOMA who suggests that property owners and managers should have access – free of charge – to whole-building aggregate monthly energy

²³ Google Initial Comments, Att. 4, "Comments of Google, Inc. in Federal Communications Commission Forum on the National Broadband Plan and Implementation of Smart Grid Technology (Oct. 2, 2009), at 4.

consumption and cost data. According to BOMA, usage information should also be provided – free of charge – to representatives of owners and tenants, and should be archived by the utility for at least five years.²⁴ Each of these requests are exceedingly burdensome and costly. As noted above, aggregating data for an entire building demands substantial manual labor and calculations by utilities, who generally do not compile, evaluate or store customer usage information in this format. Google states that "[c]ustomers and their authorized third-party service providers should be able to access home energy usage data without having to pay for the data itself."²⁵ Contrary to the assertions of BOMA and Google that this information should be provided "free of charge," the demands faced by utilities in producing and managing this data will involve significant costs. Further, given the cost implications of BOMA's requests, they should be addressed by the relevant state regulatory agencies. In addition, providing building owners and managers with tenants' energy usage information raises a number of separate privacy issues. These and similar assertions by third parties in this proceeding are troubling. Third parties desire access to and use of data for their business purposes at no expense, which will ultimately result in related costs being passed on to consumers through utility bills, effectively forcing consumers to subsidize third-party commercial activities.

²⁴ Curiously, BOMA adds that "any representative" of owners and tenants should be designated by completing a "simple request that enables them to become a 'duplicate customer of record.'" BOMA Initial Comments at 3. This request is beyond the scope of the Department's proceeding, and is more appropriately addressed by the regulatory agencies in the relevant state jurisdictions.

²⁵ Google Initial Comments, Att. 3, "Comments of Google, Inc. in Office of Science and Technology Policy Forum: Consumer Interface with the Smart Grid (March 12, 2010), at 2.

EnerNOC, Honeywell and others state that data should be available to consumers and authorized third parties directly from the smart meter itself.²⁶ While consumer and third party access to raw CEUD from smart meters has potential advantages, it presents significant concerns. As UTC notes, care must be taken to ensure that access to raw data does not create billing confusion which could undercut consumer confidence regarding accuracies of usage data. Raw data will likely lead to consumer confusion on some level, as customers attempt to compare raw usage information with data that has been verified by utilities, or try to estimate their own bills. Such confusion cannot simply be "regulated away" by state rulings that utility-verified data is supreme; raw data will still be a source of confusion for many consumers, and could result in tensions between customers and utilities. Therefore, EEI urges state regulatory authorities to carefully weigh the benefits of this practice.

Comments favoring access to raw data also overlook privacy and security issues involved with accessing information at this level. It is also important that third parties not be permitted to rely on a perceived need for direct access to raw meter data to circumvent privacy policies. Allowing such a practice would undermine state efforts to protect consumers, and would discriminate against utilities who have a long history of protecting customer privacies.

To the extent utilities enhance and audit CEUD (*i.e.*, 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), neither customers nor third parties should have a right to access such enhancements except to the extent such enhanced data is

²⁶ See Honeywell Initial Comments at 2; see also EnerNOC Initial Comments at 6-7; see also DRSG Initial Comments at 10.

provided in customer billing statement. Similarly, neither customers nor third parties (with the exception of affiliates or other entities presently relied upon by utilities internally) shall have access to energy usage data that has been aggregated.

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

In its Initial Comments, EEI stated that consumers should have access to energy price information; particularly, if dynamic pricing has been implemented in their service territory. 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. The cost for providing this level of granularity is disproportionate to the benefits.

EEI agrees with Silver Spring that providing consumers access to time-differentiated price signals is a useful approach for consumers, utilities and third parties. Time-differentiated price signals (e.g., critical peak events, 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. As Silver Spring states, "consumers are arguably more interested in knowing when to avoid peak prices, versus [] know[ing] the amount of [kWh] they have consumed" at any instant.²⁷ Customers (or their devices) should also see system emergency (*i.e.*, critical peak) signals in real time.

²⁷ Silver Spring Initial Comments at 8.

EEI agrees with NRECA that in-home Smart Grid implementation should emphasize "set and forget" controls rather than real time involvement as a measure for success.

EEI disagrees with the notion put forth by EnerNOC and Tendril that only real or near-real time information is actionable for consumers seeking to modify their energy consumption behavior. It is incorrect to state that any delay in data access can prevent participation in demand response and other programs.²⁸ As NRECA indicates, it should not be simply assumed that real or near-real time prices are necessary to support home energy services. According to NRECA, "cooperatives have used non-price-based demand response programs very successfully for more than 30 years to improve service, enhance reliability and lower energy costs."²⁹ EEI believes such efforts illustrate that Smart Grid technologies can see their intended potential without imposing costly demands on customers in order to satisfy the commercial interests of third-party providers.

EEI also disagrees with Whirlpool when it speculates that there are no additional costs to real-time information, as "the same or very similar infrastructure is required to collect and distribute information."³⁰ According to UTC, providing data to customers on a real or near-real time basis through utility networks requires major changes in utility infrastructure with significant cost implications. Further, as EEI explained in its Initial Comments, if large utilities are forced to port interval data from the utility meter to displays and/or data management systems on the customer side of the meter, the cost may

²⁸ See DRSG Initial Comments at 9-10; *see also* EnerNOC Initial Comments at 7; *see also* Tendril Initial Comments at 9.

²⁹ NRECA Initial Comments at 17.

³⁰ Whirlpool Initial Comments at 5.

be on the order of \$100-\$200 per customer or several hundred million dollars for a large utility. If short-interval (15 minutes or less) raw data must be 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, ultimately borne by utility customers, and can require substantial replacement of utility infrastructure, including infrastructure currently being built as part of Smart Grid deployments. EEI agrees with UTC that, given the costs and rate implications of data access mechanisms, decisions on access to information from utilities should be addressed by state regulatory commissions.

The cost implications of real time data access unfortunately appear to be a mere afterthought, if noted at all, for several commenters who request that significant detailed energy information be made available to consumers and third parties in real or near-real time.³¹ Again, 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 appear to want the data for their own business purposes, but wish to pass these added costs on to consumers through utility bills, thereby having consumers subsidize their commercial activities. EEI believes that consumers, for their part, have expressed little interest in or need for real-time 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

³¹ See, e.g., Honeywell Initial Comments at 1; Tendril Initial Comments at 9; BOMA Initial Comments at 4; EnerNOC Initial Comments at 7; Google Initial Comments, Att. 4, "Comments of Google, Inc. in Federal Communications Commission Forum on the National Broadband Plan and Implementation of Smart Grid Technology (Oct. 2, 2009), at 4

appliances (“prices to devices”). However none of these uses or functions requires real-time or near real-time consumption data.

The bottom line is the cost and cost allocation analyses which regulated utilities must conduct 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. Recommending or adopting policies that depart from this core principle will make Smart Grid both too expensive and the projected benefits for consumers too uncertain. This in turn will chill Smart Grid investment or in some cases create a barrier to deployment of Smart Grid technologies.

CONCLUSION

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

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: August 9, 2010