

July 12, 2010

Department of Energy
Office of General Counsel
1000 Independence Avenue, SW., Room 6A245
Washington, D.C. 20585

RE: NBP RFI: Data Access

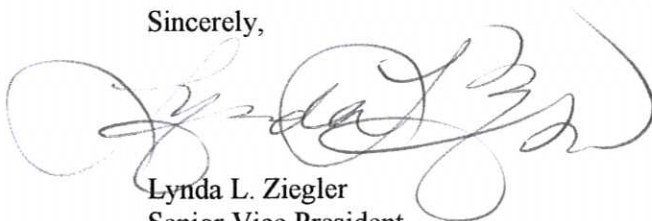
Dear Sir or Madam:

Southern California Edison (SCE) appreciates the opportunity to respond to the National Broadband Plan Data Access, Third Party Use, and Privacy Request for Information. SCE recognizes that energy information will empower customers and is a vital component of achieving the policy objectives as articulated in the National Broadband Plan.

Thus, SCE is committed to providing secure energy information consistent with the goal of providing consumers with the appropriate data they need to better manage their energy consumption. In the attachment to this letter, we provide SCE's responses to the eighteen questions asked by the Department of Energy.

We thank you again for the opportunity to provide this information, and we look forward to working with the Department of Energy, Federal Communications Commission, and other interested parties on the development of customer energy information policies.

Sincerely,



Lynda L. Ziegler
Senior Vice President
Customer Service Business Unit

SCE Responses to Customer Data Questions

1. **Who owns energy consumption data?**

SCE Response: Customer-specific data gathered or developed by a utility in the course of providing utility services is owned by the utility. Such data is subject to confidentiality and privacy requirements. In California, customers have the right to access their customer-specific information and can authorize third-party access to their information.

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

SCE Response: All customers receiving electric service from a utility should be entitled to privacy protections relating to their customer-specific energy information. Furthermore, utilities should not be required to enforce the compliance of customer-authorized third parties with privacy laws in their use of customer data because, most likely, utilities will have no ability to control or interfere with the customer's relationship with its third-party agent. The courts and state and federal agencies tasked with consumer and privacy protections are the appropriate enforcers of privacy laws, including the applicability of such protections to customer-authorized third parties.

In addition, law enforcement agencies or other authorized agents of the state or Federal Government should have access to confidential customer information with a subpoena, warrant, or as otherwise required by law.

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

SCE Response: Safeguards exist today in California to protect confidentiality of customer information collected by utilities, including statutes and California Public Utilities Commission (CPUC) mandates in regards to data security and confidentiality, and release of such data upon written customer authorization, court-ordered subpoena, warrant, or as otherwise required by law.

Additionally, SCE has recommended in the CPUC's Smart Grid Proceeding (R.08-12-009) that utilities should incorporate the Federal Trade Commission's (FTC) Fair Information Practice (FIP) principles into their respective privacy policies.

4. **Should consumers be able to opt in/opt out of smart meter deployment or have control over what information is shared with utilities or third parties?**

SCE Response: Consumers should not be able to opt in or opt out of smart meter deployments. Smart meters are an integral part of the electric grid and are foundational to achieving the national energy policies as articulated in Energy Information and Security Act of 2007 (EISA), including improvements to grid reliability and optimization, deployment of “smart” technologies, integration of “smart” appliances and consumer devices, and the provision to consumers of timely information and control options. In addition, the appropriate regulatory agencies are authorizing smart meter deployments based, in part, on the operational cost savings resulting from these smart meter deployments. Allowing customers to opt out of smart meter deployments would seriously jeopardize the achievement of such operational cost savings. In addition, SCE’s meter communication system uses a mesh network, and therefore relies on meter-to-meter communications for data transmission. Thus, allowing customers to opt out of smart meter deployment may lead to the instability of the meter communication network.

In regards to data sharing, certain data will be required in the course of providing utility services (e.g., backhailed interval usage data). Customers should not be able to restrict utility access to this data

Regardless of the data type, customers should be allowed to authorize third parties of their choosing to have access to their customer-specific usage data, and should be able to limit the scope and duration of authorized third-party access, as well as the option to terminate that access at any time.

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

SCE Response: Customers should use the existing utility and regulatory channels/mechanisms, as well as emerging communication channels to report concerns or problems with their smart meter.

6. **How do policies and practices address the needs of different communities, especially low-income rate payers or consumers with low literacy or limited access to broadband technologies?**

SCE Response: The needs of different communities are well served by universal access to data, programs, and services that allow these customers to better manage their energy consumption and lower their bills. For example, all of SCE's residential smart meters are equipped with a Home Area Network (HAN) interface that will provide customers the option to securely access near real-time energy usage data. Customers will also have access to hourly interval usage data directly through SCE's website. Customers with low literacy of, or limited access to broadband may also contact SCE's customer service representatives, 24 hours a day, 7 days a week, who can explain energy information to customers in multiple languages. Further, SCE is working with vendors to have a low cost display device available to low income and non-technical customers.

Other examples of home-to-grid technologies that serve different communities include those provided under California's Multi-Family Affordable Solar Housing and Single Family Affordable Solar Housing Programs. These programs offer fully or highly subsidized home-to-grid solar systems to qualified low-income customers or owners of low-income multi-family dwellings.

These programs and services are particularly focused on the needs of different communities, who may otherwise be unable to fund the installation of such systems in their residence or who have limited access to broadband technologies. These home-to-grid programs are designed to reduce customer energy bills without increasing monthly expenses, while promoting solutions that are expected to be both environmentally and economically sustainable.

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

SCE Response: Security standards for Smart Grid applications are critical. As stated in response to Question 10, Smart Grid security architectures need to include specific provisions (i.e. requirements) for safeguarding the confidentiality, integrity and availability of customer information in transit and at rest. Many of the security controls developed for Smart Grid applications such as encryption can be used to protect consumer privacy.

Specifically, confidentiality mechanisms and controls can and are being reused in Smart Grid technologies that interface with the customer. The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) established a DOE-sponsored public/private work group which produced Advanced Metering Infrastructure (AMI) and Automated Data Exchange (ADE) security profiles that are good examples of system and architecture requirements developed to protect customer privacy and should be followed in designing related solutions and systems. Additionally, the Smart Energy Profile 2.0 includes security architecture explicitly designed to protect customer data confidentiality.

In addition, policies regarding the collection and maintenance of customer data play an important role in the development, deployment and implementation of the Smart Grid. The increasing availability of customer information made available through Smart Grid technologies raises privacy concerns that must be appropriately addressed to safeguard customers' confidential personal or business information and privacy interests. SCE submits that appropriate safeguards exist today for customer-confidential information collected by the utilities in California -- including statutes and state regulatory mandates to maintain the security and confidentiality of such data and its release only upon written customer authorization, court-ordered subpoenas or warrants, or as otherwise required by law. SCE also supports the FTC's FIP principles for the collection and maintenance of customer data.

8. **Which of the potentially relevant data privacy standards are best suited to provide a framework that will provide opportunities to experiment, rewards for successful innovators, and flexible protections that can accommodate widely varying reasonable consumer expectations?**

SCE Response: As stated previously, SCE supports the FTC's FIP principles and national Smart Grid technology and security standards as a framework to accommodate consumer expectations.

9. **Because access and privacy are complementary goods, consumers are likely to have widely varying preferences about how closely they want to control and monitor third-party access to their energy information: what mechanisms exist that would empower consumers to make a range of reasonable choices when balancing the potential benefits and detriments of both privacy and access?**

SCE Response: Customers should have control over what customer-specific information is shared with third parties. More specifically, customers should control which third parties and how many third parties can have access to their customer-specific information. Furthermore, customers should have the option to limit the scope and duration of third-party access.

In addition, utilities can be instrumental in educating customers about the legal obligations that third parties have with respect to use of customer data, and the importance of customers transacting business with reputable entities that have appropriate privacy policies. The utilities can also provide customers with information on how they can seek redress for suspected misuse of their data by third-party agents, including filing complaints with state privacy protection agencies, the FTC, and/or the courts.

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

SCE Response: In order to protect consumer privacy, Smart Grid security architectures need to include specific provisions (i.e. requirements) for safeguarding the confidentiality, integrity and availability of customer information in transit and at rest. Many of the security controls developed for Smart Grid applications such as encryption can be used to protect consumer privacy. Specifically, confidentiality mechanisms and controls can and are being reused in Smart Grid technologies that interface with the customer. The ASAP-SG produced a DOE-sponsored public/private work group, produced AMI and ADE security profiles that are good examples of system and architecture requirements developed to protect customer privacy that should be followed in designing related solutions and systems. Additionally, the Smart Energy Profile 2.0 includes security architecture explicitly designed to protect customer data confidentiality.

11. How can DOE best implement its mission and duties in the Smart Grid while respecting the jurisdiction and expertise of other Federal entities, states and localities?

SCE Response: The DOE can best accomplish its Smart Grid mission and duties by advancing national standards for consumer data access and privacy. The states will benefit from the adoption of national standards and this would help ensure standardization and help to align the energy industry and accelerate the emerging Smart Grid.

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

SCE Response: Authorized agents of federal, state, or local governments should be able to gain access to confidential customer data through a court-ordered subpoena or warrant, or as otherwise required by law.

13. What third parties, if any, should have access to energy information? How should interested third-parties be able to gain access to energy consumption data, and what standards, guidelines, or practices might best assist third parties in handling and protecting this data?

SCE Response: Third parties acting on behalf of customers should be able to access confidential customer-specific energy information only upon written authorization of the customer. Third parties acting on behalf of the utilities to provide customer services that require access to confidential customer information should have access to confidential customer-specific energy information only pursuant to contractual confidentiality and non-disclosure obligations.

In addition, upon CPUC authorization, and consistent with current practices and for the purposes of analyzing customer usage patterns, third parties should have access to aggregated, non-customer specific usage data, as well as specific customer usage data with all identifying characteristics removed, such as name, address, and account number, such that a customer could not be recognized by the data.

In regards to how third parties should access energy consumption data, the states should adopt appropriate access rules and policies for automated data access consistent with national standards. Many state jurisdictions (including the CPUC, which has jurisdiction over the California Investor Owned Utilities (IOU)) already have established rules and procedures for providing customers or their authorized third-party agents with secure

access to energy consumption data. As such, where practicable, national standards should leverage the existing processes.

Third parties should be required by state laws to have appropriate privacy policies for the collection, maintenance and dissemination of customer-specific information. Third parties should be required to notify customers of their use of information for any purposes other than that intended by the customer in authorizing access.

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

SCE Response: In general, customers should have access to -- and should be able to authorize a third-party of their choosing to have access to -- cumulative bill-to-date usage, interval usage (provided on a day-after basis), historical usage, demand (if applicable), and near real-time usage data (provided through the HAN). Customers should determine the information their authorized third parties have access to. In addition, customers should have access to prices or charge(s) associated with the energy consumed to the extent that the information can help them manage their energy costs.

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

SCE Response: Customers should have access to the same energy information collected by the utility. Utility collection of energy usage data could be daily or less often but is not necessarily in real-time or near real-time. However, some advanced meters can measure and make available near real-time information to the customer through a HAN. SCE's advanced meter will have this capability. In that case, customers should have access to near real-time usage data provided by the HAN. In addition, state and national policies have given consideration to providing customers with near real-time presentment of retail prices. However, although presentment of this information may be desirable, the ultimate goal is to provide customers with relevant, actionable information that can help them manage their energy usage.

In jurisdictions with tiered rate structures (e.g., California), the tariff structures distort the intended affect of providing near real-time retail rates to customers. More specifically, providing near real-time pricing data to residential customers may cause customer confusion, and could even have the perverse effect of increasing overall electricity usage by

customers (e.g., an inverted tier structure provides price signals that encourage electricity usage early in the billing cycle). Thus, while tiered rates are in effect, providing near real-time pricing data is not, at this time, practicable or meaningful.

As a near-term alternative, consideration should be given to reasonable alternatives to providing customers actionable energy information. Thus, in jurisdictions where tiered rates are in affect, consideration should be given to the provision of alternative pricing information. For example, SCE intends to provide bill-to-date, bill forecast, and advanced notifications features to its residential and small business customers. Bill-to-date provides the customer's estimated bill through the current date, bill forecast provides the customer's estimated bill at the end of the billing period, and advanced notifications will provide customers notice when a preset spending target is reached.

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

SCE Response: In California, the CPUC adopted customer data confidentiality and access rules as part of its deregulation effort in the late 1990s that remain applicable today in protecting customer privacy and facilitating access by customers and third parties. For example, the CPUC has issued numerous decisions requiring the IOUs to maintain all customer-specific data as confidential and not provide that information to any third-party without the express written authorization of the customer. IOUs are generally prohibited from providing confidential customer data to law enforcement agencies in the absence of a court-ordered subpoena or warrant. IOUs are also prohibited from selling customer data. These protections remain valid with respect to the collection and maintenance of the additional customer information made available by Smart Grid technologies.

The CPUC is responsible for implementing Smart Grid policies resulting from EISA 2007 for California IOUs. As such, the CPUC has taken a number of steps to implement policies regarding Smart Grid privacy, data collection and third-party use of information. In December 2008, the CPUC instituted a Rulemaking (R.08-12-009) to determine policy in California's development of a Smart Grid system as required by EISA 2007. The scope of this rulemaking includes customer data issues, such as data privacy, security, and third-party data access. As part of this rulemaking, in December 2009, the CPUC held that the California IOUs will be required to provide customers and authorized third parties with

access to customer data in a manner consistent with EISA 2007 standards, the general public interest, and state privacy rules. The next phase of that proceeding will specifically address the rules needed to allow for data access in a manner consistent with EISA 2007 standards, the general public interest, and state privacy rules.

17. **What steps have investor owned utilities, municipalities, public power entities, and electric cooperatives taken to implement Smart Grid privacy, data collection and third party use of information policies?**

SCE Response: SCE has implemented processes for maintaining customer data as confidential and providing access to such data to third parties only upon the express written authorization by the customer, consistent with CPUC decisions and orders. SCE also has a customer data privacy policy, which informs customers of the types of information SCE collects and for what purpose. In addition, as part of SCE's smart meter deployment, SCE has designed its AMI to include security architectures to include specific requirements for safeguarding the confidentiality, integrity and availability of customer information in transit and at rest.

As part of the CPUC's Smart Grid proceeding (R.08-12-009), SCE is advocating appropriate data collection and privacy policies, as well as developing plans to implement required process and system changes to provide access to customers and authorized third parties through automated data exchange processes consistent with developing national standards. Furthermore, the next phase of the CPUC's Smart Grid proceeding will address rules to allow for data access in a manner consistent with EISA 2007 standards, the general public interest, and state privacy rules. After the CPUC adopts these rules, SCE will be better able to plan for and develop the systems and processes to implement and support the Smart Grid data policies. In addition, SCE is also engaged in the development of many security and privacy-related national standards and technology development efforts.

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

SCE Response: Consumer privacy, data accessibility and security should be considered by the DOE in evaluating Smart Grid grant applications for projects that involve the collection and sharing of customer data. SCE notes that utility customer data practices are also subject to state statutes and regulatory mandates. Thus, any DOE evaluation should give appropriate consideration to existing state requirements.