Florida Power & Light Company, 700 Universe Blvd. Juno Beach 33408
Telephone: (561) 691-2790, Fax: (561) 691-7577

FPL

July 12, 2010

U.S. Department of Energy,
Office of the General Counsel
1000 Independence Avenue, SW
Room 6A245
Washington, DC 20585
Via Email: broadband@hq.doe.gov

Re: U.S. Department of Energy Request for Information Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy

A. Introduction

A wholly-owned subsidiary of NextEra Energy, Inc., Florida Power & Light Company (FPL) is a public utility incorporated in the State of Florida that provides wholesale and retail electric service. It is one of the largest and best-performing electric utilities in the nation, serving approximately 4.5 million customer accounts and delivering electricity to more than 8.8 million people. FPL owns and maintains 73,700 miles of transmission and distribution lines in Florida.

FPL is implementing one of the largest smart meter deployments in the country incorporating 4.5 million smart meters. FPL has been awarded a $200 million American Recovery and Reinvestment Act Smart Grid Investment Grant from the U.S. Department of Energy (DOE) to help support its "Energy Smart Florida" plan to deploy Smart Grid technologies. FPL customers expect affordable, reliable, clean-energy solutions now and in the future, and FPL is committed to meeting this expectation by investing to make its infrastructure stronger, smarter, cleaner, and more efficient. The utility currently has the lowest residential rates of all 55 utilities in the state of Florida and service reliability significantly better than the national average.

FPL respectfully submits the following comments in response to the DOE's Request for Information (RFI) on Data Access, Third Party Use, and Privacy. (75 Fed. Reg. 26,206 (May 11, 2010)).

B. Executive Summary

FPL and most utilities have policies that protect consumer privacy by treating customer data, energy usage data and all other data as confidential. The smart devices that are now being added to utility infrastructures expand the scope of customer data that will now be

available, but do not change the importance of continuing to treat this data in a confidential manner. If anything, the additional data makes it even more important to reassure customers that the utility industry will continue to protect the privacy and safeguard the rights of our customers to have their data protected and kept confidential. Only if we receive explicit and verifiable customer authorization to release customer data to a third party will we do so.

Smart Grid technologies offer significant customer benefits. As the DOE recognizes, Smart Grid deployments and their benefits have the potential to be "lost or substantially delayed" if consumers lack confidence in Smart Grid technologies due to perceived privacy risks associated with sensitive information derived from energy consumption data.[1] With that in mind, FPL appreciates the opportunity to provide DOE with information about FPL's existing processes for providing customer access to energy consumption data while ensuring strict privacy protections of said data.

Protection of customer-specific data has historically been the role of the utility and it is a role that FPL takes very seriously. As more and more Smart Grid resources become available on FPL's distribution system, FPL will continue to implement tight controls and adapt its processes to protect the privacy of its customers' data. At the same time, FPL has also taken a pro-active approach to customer education, including investments in educational materials, web-based systems, and other tools to help customers better understand and utilize energy consumption data made available by Smart Grid technologies.

FPL believes the development and implementation of effective Smart Grid technologies can be achieved in conjunction with protecting consumer data information. To meet the U.S. policy objective established under the Energy Independence and Security Act of 2007, (i.e., "*to maintain a reliable and secure electricity infrastructure that can meet future demand growth*"), constant review and analysis of consumption data is required in order for the utility to maintain system reliability and power quality. As a result, the utility must continue to control aggregated system operational data to ensure system reliability. In addition, the utility is also best situated to be the custodian of individual customer energy consumption data.

The utility does not have an inherent commercial business interest to resell and disseminate customer-specific consumption data; rather, the utility's interest is to provide the customer access to consumption data generated from the infrastructure the utility owns and operates, such as smart meters and protecting the privacy of that data at all times. Moreover, FPL is governed by the consumer privacy laws of the state of Florida and is prohibited from releasing or sharing customer data with third parties without the explicit consent of the customer or pursuant to a valid subpoena.

---

[1] 75 Fed. Reg. 26,203 at 26,204.

C. FPL Responses

Question 1: ***Who owns energy consumption data?***

The utility, acting as an integrated utility or as the distribution company for deregulated markets, has ownership rights to aggregated system operational data to ensure system reliability. While the utility owns the metered infrastructure, FPL believes the customer should have access to their specific energy usage data as metered at the customer's premises in time intervals as reported by FPL to the customer. The utility has historically been the steward of individual customer energy consumption data. Individual customers have privacy rights in their individual data, and the utility has a corresponding obligation to protect against unauthorized disclosure of that data. The customer also has the right to authorize the release of his or her individual energy consumption data to third parties, including retail service providers in deregulated markets. However, the utility must continue to have access and control over customer energy consumption data for utility functions. Subsequently, non customer-specific operational data should remain the property of the utility.

As the customer's service provider, FPL is governed by existing Florida customer privacy laws that preclude FPL from releasing any customer data to a third party without the express consent of the customer unless otherwise provided by Florida or Federal law or pursuant to a valid subpoena. This pertains to customer specific energy use and price data. A customer who files a complaint with the Florida Public Service Commission (FPSC) may waive his or her privacy rights depending upon the manner in which that complaint is filed. These general rules and principles have applied in the past and continue to apply as smart meters are deployed.

In this era of heightened focus on cyber security, FPL has enhanced its existing systems to prevent unauthorized entities from accessing sensitive customer data. In order to continue to maintain system reliability and effectively plan for system needs, the utility must continue to maintain the energy usage data for real-time system assessments. The utility has the obligation to safeguard and protect sensitive customer data it generates from infrastructure it owns and operates, such as smart meters. FPL takes this obligation seriously. Utilities have continued to develop tight controls and protocols to eliminate inappropriate distribution of the data, both to internal and external parties. It is not in the customer's or FPL's interest to relax this requirement.

In the end, the critical policy issue is not who owns energy consumption data. Instead, the more relevant issues at hand are ensuring customers' privacy rights are safeguarded and that customers are provided access to and assistance in the usage of energy consumption data, which utilities are best equipped to continue to provide.

Florida Power & Light Company, 700 Universe Blvd. Juno Beach 33408
Telephone: (561) 691-2790, Fax: (561) 691-7577

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

The utility's residential, commercial and industrial customers whose energy information data is currently being safeguarded and protected by the utility should be entitled to privacy protections relating to energy information.

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

It is our viewpoint that the utility has the obligation to safeguard and protect sensitive customer data it generates and has in its possession from infrastructure it owns and operates, such as smart meters. FPL takes this obligation seriously. Utilities have continued to develop new and enhance existing tight controls and protocols to eliminate inappropriate or unauthorized release of the data, both to internal and external parties. It is not in the customer's or FPL's interest to relax this requirement, which could subject the customer to loss of security and privacy and subject FPL to potential liability.

Moreover, before FPL will release individual customer data to a third party, the customer must request that their data be shared with specific companies, entities or third party agents authorized to act on their behalf. Third parties that receive customer authorization to receive customer-specific energy consumption data should be required to obtain explicit customer approval prior to reselling or distributing that data. The authorized third party or agent must be required to extend all requisite privacy protections and be held responsible and liable for any unauthorized access to that data. FPL is governed by existing Florida customer privacy laws that preclude FPL from releasing any customer data to a third party without the express consent of the customer unless otherwise provided by Florida or Federal law or pursuant to a valid subpoena. This pertains to customer specific energy use and price data. The third party has the obligation to protect the data that is shared with them and the utility does not share in that obligation.

Question 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?***

In order to achieve benefits of the Smart Grid, smart meters must be widely deployed to all consumers and consumers should not have an option to opt out of deployment. Any option to opt out of a smart meter deployment would require utilities to maintain dual processes and systems and not allow the benefits of smart meters to be obtained. This would ultimately result in higher costs to consumers.

Customers will receive the benefits from network modernization afforded by deployment of Smart Grid technology. Upon Smart Grid deployment, there will be many benefits to the customer, (*i.e.*, improved power quality, increased reliability, increased safety, faster service restoration, increased utility productivity).

Consumers will have options to participate in programs enabled through smart meters as authorized by the bodies that regulate the utilities. The consumer should have full control over what is shared with third parties. The customer has the right to authorize the release of his or her individual energy consumption data to third parties.

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

All mechanisms currently in place to report utility concerns should be made available and leveraged to facilitate reporting of concerns or problems with the smart meters. These channels include phone calls, emails, and letter correspondence to the utility or directly to the consumer advocate or public service commission that has advocacy responsibilities for the consumers.

Question 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?***

Smart Grid technologies will provide FPL's Customer Care Centers with improved information about the consumer and their power use, streamlining inquiry resolution for all customers, irrespective of access to broadband technologies.

As Smart Grid technologies are more widely deployed, they will spur innovation in developing products and services targeted to customers with unique needs and requirements. For example, FPL is testing home energy monitors and controllers that would use information from smart meters to help customers easily manage their energy usage. In addition, FPL is exploring offering customers the ability to receive alerts when their electricity usage reaches levels established by the customer. Clearly, the enhanced ability to monitor energy usage and act on this information has important benefits for low-income customers in particular.

Smart Grid technologies enable utilities to optimize operations - helping FPL customers better manage their bills and keep service reliability high over the long term. Standards-based Smart Grid solutions could commoditize technologies, enable economies of scale and deliver cost effective energy management tools to benefit all consumers.

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

FPL is governed by existing Florida customer privacy laws. Historically, the States have been responsible for privacy regulation of customer data, (e.g., developing

various data privacy protections, access and disclosure laws and regulations for customer energy consumption data and other customer information).

Although still in draft form at this time and subject to change, FPL believes the National Institute of Standards Technology's (NIST) initiatives to develop Smart Grid Standards that protect privacy and the confidentiality of personal information are relevant. Section 7.3.3 of the NIST Framework and Roadmap for Smart Grid Interoperability recognizes that the privacy implications of Smart Grid continue to evolve and designates the Cyber Security Coordination Task Group (CSCTG) as the focal point for developing Smart Grid privacy policy at this time.

- In Section 4.1 of NIST's Draft Smart Grid Cyber Security Strategy and Requirements (NISTIR 7628), CSCTG identifies the following categories of privacy principles applicable to Smart Grid: management and accountability, notice and purpose, choice and consent, collection and scope, use and retention, individual access, disclosure and limiting use, security and safeguards, accuracy and quality, as well as openness, monitoring and challenging compliance.

FPL believes that the NIST position and Fair Information Practice Principles, which serve as the basis for the Department of Homeland Security's Privacy Policy, should guide the DOE in developing data-privacy standards for Smart Grid development, deployment and implementation. Largely similar to CSCTG findings, the Fair Information Practice Principles of transparency, individual participation, purpose specification, data minimization, use limitations, data quality and integrity, security, accountability and auditing are especially applicable to Smart Grid development, deployment and implementation, where access to personally identifiable information is necessary to provide the more advanced, efficient and uniquely manageable energy services that Smart Grid allows.

Consistent with the National Association of Regulatory Utility Commissioners' position in its *Resolution Urging the Adoption of General Privacy Principles For State Commission Use in Considering the Privacy Implications of the Use of Utility Customer Information*, FPL also believes that because private, customer information, when shared with joint ventures or independent contractors, inherently becomes more vulnerable to unauthorized use, a regime where customers must provide affirmative express consent before the utility or service provider shares any of the customer's confidential information with affiliates or third parties is best suited for the development, deployment and implementation of Smart Grid.

FPL also agrees with the CSCTG conclusion that a current lack of consistent and comprehensive privacy policies and standards throughout the states, government agencies, utilities and other entities involved in Smart Grid management, information collection and use represents a significant privacy risk that must be addressed.

FPL's position is that, at this time, the NIST CSCTG appears to be effectively developing comprehensive, end-to-end policies and standards for Smart Grid privacy

and protection of personal information that have uniform application to all utilities and service providers. FPL encourages the DOE to allow the standards development process to continue at NIST and consider the resulting recommendations.

Due to the similarities in recent advocacy, regulatory and enforcement efforts related to privacy regulations governing telecommunications and internet carriers, FPL believes such federal regulations could also serve as a guide in the development, deployment and implementation of Smart Grid to maintain customer privacy, while enabling emerging technologies to flourish.

Question No. 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?***

Smart Grid Privacy Standards are a work in progress from a regulatory, legislative and technical perspective. A successful data privacy strategy must incorporate best practices, policies, and state / federal laws that protect consumer interest – backed with strong technical standards.

FPL's position is that, at this time, the NIST Cyber Security Working Group is the most effective forum to develop comprehensive, end-to-end policies and standards for Smart Grid privacy and protection of personal information. FPL believes that an open process, with participation from all stakeholders is the best approach to protecting customer privacy and personal information, while enabling innovation and new business opportunities from the deployment of a national Smart Grid.

Question No. 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?***

Consumer demand for new energy services will vary by demographics, usage, geography and other factors. To foster innovation and develop this market, FPL strongly believes in a layered technical architecture that provides a common foundation while enabling consumer driven demand and preferences in the marketplace to pick winning products and technologies. Let market competition pick the physical communications infrastructure within the premises, similar to the way consumers pick DSL, Cable and other Internet connections today; customers may make different choices based on functionality, cost, geography and other factors.

Additional recommendations include;

- Standardize on a common communications layer based on Internet Protocol (IP) to enable the interaction of a diverse set of technologies and products.
- Leverage standards development organizations to define common messaging formats to enable the exchange of energy information.

However, utilities must have the opportunity to determine what mechanism(s) is best suited to perform the functionality needed to empower consumers.

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

While it is difficult to predict with any specificity security architecture provisions that should be built into Smart Grid technologies, a comprehensive approach to protecting consumer privacy must deliver a layered and coupled solution integrating all components:

a. Data Privacy - Policy, Best Practices, Risk Assessment, Mitigation Plan, Applicable Federal and State Laws

b. Comprehensive Smart Grid Security Architecture

Smart Grid technologies' security architecture should take a "defense-in-depth" approach offering multiple layers of defense across the entire architecture (from the end-point device, to the interconnecting mesh network, to the back-office systems) to ensure the privacy of consumer data. Given that the technologies (and the implementation of said technologies) will most likely come together in a variety of combinations, the best approach is to create baseline security standards and capabilities for each component and ensure the security interoperability between the various components of a Smart Grid system. This methodology is already being developed through the efforts of NIST, and FPL strongly encourages that DOE support those efforts and adopt the recommendations of NIST as they relate to aforementioned issues.

Question No. 11: ***How can DOE best implement its mission and duties in the Smart Grid while respecting the jurisdiction and expertise of other Federal entities, states and localities?***

DOE is in the position to help facilitate the coordination that must take place amongst and between all the various entities. Congress has given a number of federal entities authority over certain aspects of Smart Grid. As a result, it is imperative that the respective federal, state, and local agencies work cooperatively to achieve the best possible outcomes for jurisdictional customers and the nation as a whole.

However, federal regulators must not make decisions of this magnitude in a vacuum without a discussion of the costs involved, value to the customers, protection of customer privacy and a clear understanding of how those costs will be recovered.

Question No. 12: When, and through what mechanisms, should authorized agents of Federal, State, or local governments gain access to energy consumption data?

At the present time, FPL seeks confidential classification from the Florida Public Service Commission when individual customer data (otherwise considered private

and confidential) must be disclosed or produced by FPL pursuant to a valid request in the regulatory setting. In the event of similar requests at the federal level, FPL would endeavor to obtain the same type of protection. At the local government level, FPL is sometimes required to make customer usage data available, (e.g., for audits undertaken in the context of franchise agreements, Municipal Utility Tax issues, and perhaps others), but the Company does not allow that data to be taken from the Company's premises. Further, efforts should be undertaken to redact any information that would otherwise allow for a link to be made between data or information and the specific customer, as that data becomes a public record once in the possession of the local government entity.

To that end, government entities should not have direct access to customer data. To the extent certain information disclosure is required by law or regulatory process, utilities will continue to cooperate with authorized government entities as they do today. The data should be aggregate in form and provided through standard reporting mechanisms.

Question No. 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?***

The utility should not provide individual customer data to third parties, except at the explicit request of the customers or as otherwise provided by Florida or Federal law or pursuant to a valid subpoena. The customer must request that their data be shared with specific companies, entities or third party agents authorized to act on their behalf. Any such data should be provided in the standard utility format using the utility's standard interfaces and data format.

As the customer's service provider, FPL is governed by existing Florida customer privacy laws that preclude FPL from releasing any customer data to a third party without the express consent of the customer or as otherwise provided by Florida or Federal law or pursuant to a valid subpoena. This prohibition applies to customer-specific energy use and price data and should extend to all third parties authorized to receive customer data. Third parties authorized to receive customer data should be subject to disclosure requirements and required to share with utilities data protection responsibilities, which must include all liabilities resulting from any unauthorized access to customer data.

Lastly, authorized third parties must be required to obtain affirmative consent from the customer prior to reselling or disseminating their individual consumption energy usage data. Further, third parties authorized to receive customer data should be subject to disclosure requirements and liable for all resulting liabilities from any unauthorized access or disclosure of customer data.

Question No. 14: What forms of energy information should consumers or third parties have access to?

Consumers should be provided the information from the meter that is used to calculate their usage which is used to determine the billing. This should also include interval usage information collected by the utility that can be used by the consumer to understand their usage history to make smart decisions about future usage. If the consumer provides consent, this same information can be made available to a third party. Any such data should be provided in the standard utility format using the utility's standard interfaces and data format.

Third parties authorized by the utility customer should only have access to the same type of energy information provided to the utility customer. Furthermore, third parties should not have any rights to access aggregated customer usage data or aggregated system operational data. And, to the extent utilities enhance customer energy consumption data using software programs and other systems for varied internal purposes, 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 statements. 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 customer usage data or aggregated system operational data.

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

While the utility owns the metered infrastructure, FPL believes the customer should have access to their specific energy usage data as metered at the customer premises in time intervals, as reported by FPL to the customer.

While FPL supports innovation and new services aimed at enhancing the customer's utility service experience, it must not be overlooked that the primary role of the power meter is to measure power consumption at the premises level - broadening the meter's role into a complex consumer communications gateway could significantly increase capital and operating costs for utilities and ultimately customers.

FPL believes that any architecture or design providing real-time or near-real time electricity usage should be reliable and cost-effective to consumers. The delivery of real-time data will increase utilities' capital and operating costs and ultimately be borne by the customer; it is important for the utility to identify the appropriate investment level that should be based on informed discussions with all stakeholders about value and cost. Specific implementations may vary based on state and community preferences with respect to cost, reliability, ease of use and functionality.

The electric utility's primary function is to provide safe, secure, reliable and cost effective electricity to all customers; it is incumbent upon the utility to focus on these priorities and fully understand the impact of alternative uses of the energy infrastructure on overall system reliability and cost to the customer.

Question No. 16: ***What steps have the states taken to implement Smart Grid privacy, data collection, and third party use of information?***

The Florida Public Service Commission (FPSC) has implemented policies and practices that uphold existing Florida customer privacy laws that preclude FPL from releasing customer-specific data to a third party without the customer's consent unless otherwise provided by Florida or Federal law or pursuant to a valid subpoena. The FPSC has not implemented any steps at this time specifically directed at implementation of Smart Grid privacy, data collection and third party use of information.

Question No. 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?***

For years, FPL has had processes and procedures in place to protect sensitive customer data and provide third party access to that data. While Smart Grid, or more specifically "smart meter-generated data", is a new phenomenon, the duty of maintaining the integrity and privacy of customer data is not different from what it has been and will continue to be the highest priority for FPL and other electric utilities.

FPL considers the safe delivery of electrical service our paramount priority. This includes the protection of our networks and customer data. FPL's standards are much stricter than the current industry standards, and we are taking a very methodical approach to our rollout of smart meters. We did not roll out smart meters until we could ensure our customers the same high standards and level of privacy protections as historically provided.

Question No. 18: ***Should DOE consider consumer data accessibility policies when evaluating future Smart Grid grant applications?***

In considering this question, the DOE should recognize that some of the Smart Grid Investment Grant awards involve comprehensive multi-level Smart Grid infrastructure deployments. These projects include deployment of relays, synchrophasors and phasor measurement units and that have little to do with the equally important installation of smart meters on household and industrial structures where the customer-specific consumption data is created. No customer-specific data is created by technological improvements to FPL's grid delivery system, which are, generally speaking, installed and located away from end-users.

Therefore, such a requirement is premature and makes little sense for future grant applications that may not include smart meter devices or where such devices that

collect and generate customer data may only be a small subset of the DOE Smart Grid request for grant award. Broadly worded restrictions that apply to all grant applications could result in delays in the development and deployment of Smart Grid technology.

Thank you for your consideration of these comments.

Respectfully Submitted,

Chris Bennett
Executive Vice President Business Strategy & Policy
NextEra Energy, Inc.
700 Universe Blvd
Juno Beach, FL 33408
561-691-7460
Chris.Bennett@fpl.com

Tonja Wicks
Manager, Regulatory Issues
Florida Power & Light Company
700 Universe Blvd
Juno Beach, FL 33408
561-691-2790
Tonja.Wicks@fpl.com

July 12, 2010