Q.

1. What jurisdiction does the Florida Public Service Commission (FPSC) have over smart meters?

A.

The FPSC has jurisdiction over smart meters consistent with the jurisdiction it has always exercised over all other commercially acceptable measuring devices and meters. The use of smart meters does not in any way alter the jurisdiction of the Commission.

The Commission's jurisdiction over smart meters falls within the broader grant of authority by the Florida legislature found primarily in sections 366.03, 366.04, and 366.05, Florida Statutes. Those statutes include the following grants of authority and jurisdiction which are directly applicable to the question posed:

§366.03, Florida Statutes: "Each public utility shall furnish to each person applying therefor reasonably sufficient, adequate, and efficient service ***upon terms as required by the commission.*** "

§366.04(1), Florida Statutes: "In addition to its existing functions, ***the commission shall have jurisdiction to regulate and supervise each public utility with respect to its rates and service***"

§366.04(5), Florida Statutes: "***The commission shall further have jurisdiction over the planning, development, and maintenance of a coordinated electric power grid throughout Florida*** to assure an adequate and reliable source of energy for operational and emergency purposes in Florida and the avoidance of further uneconomic duplication of generation, transmission, and distribution facilities."

§366.05(1), Florida Statutes: "***In the exercise of such jurisdiction, the commission shall have power to prescribe fair and reasonable rates and charges, classifications, standards of quality and measurements,*** including the ability to adopt construction standards that exceed the National Electrical Safety Code, for purposes of ensuring the reliable provision of service, and service rules and regulations to be observed by each public utility; to require repairs, improvements, additions, replacements, and extensions to the plant and equipment of any public utility when reasonably necessary to promote the convenience and welfare of the public and secure adequate service or facilities for those reasonably entitled thereto; to employ and fix the compensation for such examiners and technical, legal, and clerical employees as it deems necessary to carry out the

provisions of this chapter; and to adopt rules pursuant to ss. 120.536(1) and 120.54 to implement and enforce the provisions of this chapter."

The Florida Administrative Code includes a number of provisions that regulate and provide for the testing of meters and metering devices. Included within that body of administrative regulations is Rule 25-6.049, F.A.C., which provides in pertinent part as follows: ***"All energy sold to customers shall be measured by commercially acceptable measuring devices owned and maintained by the utility."*** Provided the meters owned and maintained by the utility are "commercially acceptable", they satisfy the requirements of the Florida Administrative Code.

Pursuant to its authority, the Commission has already exercised its jurisdiction over FPL's smart meters and smart meter program in a number of different settings. In Order No. PSC10-0153-FOF-EI issued March 17, 2010 in Docket No. 080677-EI, the Commission formally approved FPL's smart meter program and found as follows (at page 140 of the cited Order):"The (FPL) AMI project is prudent and should not be delayed." In that same Order, FPL was directed to file annual progress reports in the Energy Conservation Cost Recovery docket to provide updates on the implementation of smart meters. FPL has filed those annual reports on March 21, 2011 (in Docket No. 110002-EG) and on March 21, 2012 (in Docket No. 120002-EG). The Commission has also exercised its jurisdiction over meter enclosure repair and replacement issues associated with FPL's smart meter program when it entered Order No. PSC-11-0194-DS-EI on April 13, 2011 in Docket No. 110033-EI. Additionally, the Commission has exercised its jurisdiction over this program when it entered Order No. PSC-11-0257-TRF-EG in Docket No. 110031-EG on June 13, 2011. That Order approved FPL's proposed residential dynamic price response pilot rate and associated tariffs which were implemented pursuant to the Department of Energy $200 million grant received by FPL under the American Recovery and Reinvestment Act associated with FPL's Energy Smart Florida project. FPL subsequently filed its required annual report on this program on May 24, 2012 in Docket No. 110031-EG.

Finally, we would like to address questions about mandatory time-of-use rates or mandatory energy management programs. We already have voluntary time-of-use rates available to both business and residential customers, and we do not plan to propose mandatory time-of-use rates just because we have installed smart meters.

FPL conducted a pilot (approved by the Commission) to assess in-home energy management technologies, such as home energy controllers. As part of this pilot we also tested a voluntary dynamic pricing program and the results will be provided to Staff by April 30, 2013.

The introduction of any new rates would need to go through the regulatory process and ultimately be approved by the Commission. If offered in the future, we feel very strongly that any such program should be voluntary.

Q.

2. What other State/Federal/Trade organizations have jurisdiction over smart meters and what are their responsibilities?

A.

The Federal Communications Commission ("FCC") has jurisdiction over the communications aspects of the meter. This includes the obligation to establish exposure limits that ensure that FCC-regulated transmitters do not expose the public or workers to levels of RF energy that are considered by expert organizations to be potentially harmful. This jurisdiction is conferred on the FCC by the Communications Act of 1934. Pursuant to this jurisdictional grant, along with additional direction provided by Congress in the Telecommunications Act of 1996, the FCC adopted limits for Maximum Permissible Exposure (MPE) based upon a detailed study and analyses including criteria published by the national Council on Radiation Protection and Measurements (NCRP) and by the American National Standards Institute/Institute of Electrical and Electronics Engineers, Inc. (ANSI/IEEE). U. S. Circuit Courts of Appeal have considered this issue in the context of cell phone litigation and determined that the doctrine of Federal Conflict Preemption applies in this situation, such that the MPE standards established by the FCC control.

In a letter dated July 6, 2012 from Julius Knapp, Chief of the FCC Office of Engineering and Technology, to Mark Goldstein, Director of Physical Infrastructure Issues for the U.S. Government Accountability Office, Mr. Knapp wrote as follows: "The [FCC] Commission staff has continuously paid close attention to developments related to RF exposure and has worked closely with other federal agencies with health expertise such as the Food and Drug Administration. At this juncture, we believe our current standards are appropriate and protect the public against the possible harmful effects of RF exposure. However, we appreciate that it has been many years since the Commission conducted a formal review of the current standard." As a result, the FCC staff has recently presented to the Commission a proposed rulemaking to review the current standards.

Additionally, in the specific case of FPL's smart meters, Julius P. Knapp, Chief of the FCC Office of Engineering and Technology, wrote to Florida Senator Bill Nelson on July 17, 2012 and stated in pertinent part as follows: "In the case of smart meters, we note that FPL correctly cites in its fact sheet that [t]he Federal Communications Commission (FCC) has set limits on the maximum permissible exposure for emissions of RF-emitting devices. These limits are well below the point at which known biological impacts occur, and the smart meters being installed by FPL operate at levels that are hundreds of times lower than the FCC limit."

Other than the FCC jurisdiction over the communications, the American National Standards Institute (ANSI) dictates the other requirements of the meter. Other organizations, such as National Electrical Manufacturers Association (NEMA) and the Institute of Electrical and Electronics Engineers (IEEE) all roll up through the ANSI standards.

On the privacy issues, the Federal Trade Commission has well established provisions that directly address the protection of non-public information. Additionally, federal and state law is also applicable. In addition to these sources and the specific information provided in response to question 8, FPL would add that protecting the confidentiality of customer information has always been a top priority, and we continue to diligently protect against unauthorized disclosure of customer specific data and information.

See response to question 8 below.

Q.

3. Are transmitters utilized by smart meters licensed by the Federal Communications Commission (FCC)? How does a utility or transmitter manufacturer comply with FCC radio frequency (RF) emission requirements?

A.

As filed in FPL's response to question 8 in the Smart Meter Data Request #1 - All communication radios within the smart meters installed by FPL operate within the Industrial, Scientific & Medical (ISM) bands and comply with all applicable FCC regulations. Silver Spring Networks, the company that produces the communication radios within the meter, performed testing of the levels of radio frequencies emitted by the transmitters and filed the results of these tests with the FCC to show compliance with the FCC standards. In addition, General Electric, the meter manufacturer, has conducted American National Standards Institute (ANSI) tests confirming that the radio frequencies emitted by the transmitters within the smart meters meet all applicable FCC requirements. FPL also retained an independent third party RF regulatory and engineering consulting firm, Sitesafe, that conducted field testing and has confirmed that FPL's smart meters emit radio emissions at levels significantly below the standards established by the FCC.

Also see FPL's response to questions 11 & 12 in the Smart Meter Data Request #1.

Q.

4. Have the potential health effects from RF from wireless smart meters been studied?

A.

As filed in FPL's response to question 9 in the Smart Meter Data Request #1 - The relevant standards for radio frequency (RF) transmission are established by the Federal Communications Commission (FCC) based on their analytical acceptance of relevant studies and information. FPL has reviewed and studied a number of independent reports and continues to monitor and study new reports conducted by other entities in the regulatory, scientific and medical communities. These efforts, together with testing that has been performed on FPL smart meters and their component parts have consistently confirmed that FPL's smart meters and related devices operate at levels significantly below the standards established by the FCC. In fact, the smart meters that FPL is installing operate at levels hundreds of times lower than the limit established by the FCC. Regarding average transmission times, FPL smart meters transmit on average less than two total minutes a day for all their communications, which includes non-usage transmissions for system alerts and network management.

See materials in FPL's response to question 33 Smart Meter Data Request #1 for more information on RF studies.

Q.

5. Have the effects of RF from a multi-meter installation been studied?

A.

As filed in FPL's response to question 12 in the Smart Meter Data Request #1 - In a November 2010 study, Electric Power Research Institute (EPRI) field tested exposure levels from a bank of 10 smart meters of 250 mw power level at one foot distance in order to simulate a bank of smart meters located at a multi-family building, such as an apartment house. The exposure level was below the FCC standard, equivalent to only 8% of the standard. In the same study, EPRI measured exposure of one smart meter from eight inches behind the meter panel box in order to simulate proximity on the opposite site of the meter wall. At 5% duty cycle (trasmittting 5% of the time) it yielded an exposure of only 0.03% of the FCC standard. Even at 100% duty cycle (i.e., always transmitting), exposure at eight inches behind the smart meter was 0.6% of the FCC limit.

FPL also contracted with Sitesafe Inc. an independent third party radio frequency (RF) regulatory and engineering consulting firm, to evaluate the RF emissions from FPL's Smart Meters. Sitesafe measured the power density of the wireless components of the network and compared those measurements to levels regulated by the Federal Communication Commission (FCC). The power density of all the equipment tested significantly below the permissible regulatory limits.

Within this study, multi-smart meter installations were also evaluated. The study indicates that the cumulative effect of multiple smart meters mounted at the same location is simply a linear addition of emissions. The study concludes that even if a person could get within one foot of 100 smart meters, the exposure would only be 14.1% of the permissible exposure limit, or well within the FCC limits.

See Sitesafe report attached to FPL's response to question 11 in the Smart Meter Data Request #1.

Q.

6. What is the FCC's approval process for a smart meter transmitter?

A.

FCC's approval process for RF emitting devices can be found under FCC CFR 15.247 regulations.

FPL expects all vendors to meet FCC requirements in regards to smart meters and utilization of the ISM spectrum. We also verify compliance by acquiring and reviewing the SSN NIC filing directly from the FCC website. Ultimately, it is the meter vendor that needs to go through the process of approval with the FCC, and FPL has requested SSN to respond with further details to this question.

Q.

7. Does the utility consider individual customer data confidential?

A.

As filed in FPL's response to question 15 in the Smart Meter Data Request #1 - Yes. The Company designates certain customer-related data as either "non-public information" ("NPI") or confidential. NPI are those data elements required to be protected by law (State and/or federal), such as customer financial data and social security numbers, to protect against identity theft and other illegal activity by third parties. Other personal customer data, such as addresses, emails, telephone numbers, customer account numbers, billing history, and electric usage data when linked to any other identifying information, are treated as confidential pursuant to Company policy in order to protect the customer's privacy. It is important to emphasize that FPL smart meters do not store or transmit any personally identifying information.

Q.

8. What is the legal basis for the utility's privacy policy?

A.

The Company designates certain confidential customer-related data as either Non-Public Information ("NPI") or Personally Identifiable Information ("PII"). NPI are those data elements required to be protected by law (State and/or Federal), such as customer financial data and social security numbers, to protect against identity theft and other illegal activity by third parties. Other personal customer data, such as addresses, emails, telephone numbers, customer account numbers, billing history, and electric usage data when linked to any other identifying information, are PPI and are treated as confidential pursuant to Company policy in order to protect the customer's privacy.

The Company's privacy policy is consistent with a number of state and federal laws and regulations. On the federal side, the following provide guidance and support for FPL's policies: the Federal Trade Commission Act; Fair Credit Reporting Act; Fair and Accurate Credit Transactions Act; Electronic Fund Transfer Act; Driver's Privacy Protection Act; Electronic Communications Privacy Act; Health Information Portability & Accountability Act; Americans with Disabilities Act; and the FTC "Red Flags" Rules. On the state side, the following statutes, along with the common law, support FPL's policies: §501.0118, Florida Statutes; §540.08, Florida Statutes; and §817.5681, Florida Statutes. Additionally, in the context of FPL's proceedings before the FPSC, when required to provide confidential customer information in its filings and/or in response to discovery or data requests, FPL requests confidential classification of such NPI and/or PII pursuant to §366.093, Florida Statutes.

During the Smart Meter Workshop Staff also asked about the status of Congressional action concerning cyber-security. The Cyber Security Act of 2012 (S. 3414) failed to move forward in Congress after the Senate fell short of the 60 votes needed to "invoke cloture" (i.e. stop debate) on August 2. In its current form, the Cyber Security Act of 2012 had the following provisions to address truly critical cyber infrastructure:

- Define covered critical infrastructure
- Create Interagency task force with relevant government agencies as equal partners
- Authorize general inventory of covered critical infrastructure
- Establish Information Sharing & Analysis Center-selected private sector advisory committees

- Create private sector process to recommend critical infrastructure "baseline performance goals"
- Create a voluntary incentive program for operators of covered critical infrastructure that meet these goals

FPL continues to closely monitor this issue.

Q.

9. Does the utility share individual customer data with others, including affiliates?

A.

As filed in FPL's response to question 16 in the Smart Meter Data Request #1 - FPL will only share confidential customer data with other parties, including affiliates, to the extent necessary to meet legitimate business needs (for example, utilization of a collection agency for delinquent accounts). In such cases, FPL takes steps to ensure those other parties also protect the confidentiality of the information disclosed. Absent a legitimate business purpose for sharing confidential customer data, FPL will only disclose such information upon the customer's explicit authorization or as required by law.

Q.

10. What customer information is stored with the utility for a period of time that is longer than necessary to bill the customer?

A.

Customer information such as name, address, phone number, social security number, bill account number, customer number, and energy usage history data are retained for five years in accordance with FPL data retention policies and then purged from the system. While retained, this data is protected and treated as confidential pursuant to FPL policy in order to protect the customer's privacy.

Q.

11. Can a smart meter identify the usage patterns of specific devices within a customer's home or business?

A.

Smart meters only measure how much energy the premise is using, and the data FPL smart meter's collect cannot identify the usage patterns of specific devices within the customer's home or business.

Q.

12. What cyber security measures has the utility taken to ensure the security of the data transmitted by the meter?

A.

It is important to emphasize that FPL smart meters do not store or transmit any personally identifying information.

The data transmitted from the smart meter, which has no personally identifiable information, back to the FPL back office is encrypted to provide end-to-end data privacy, while advanced data protection processes provide message integrity and authentication between devices participating in the mesh network. So, even if someone succeeds in intercepting data coming off a smart meter, that data will be of no use as it is encrypted.

In addition, FPL has taken an industry leading position to secure the data on the network. The data transmitted by FPL's smart meters traverses several different networks starting with the mesh network comprised of the meters, relays and access points (APs) which are all owned by FPL. Once the data reaches the AP, it is sent across public cellular networks (still encrypted) to the FPL back office, where the back office applications collect, decrypt and process the incoming data. Finally, the data enters the FPL corporate network, where it is stored and used for business purposes.

Q.

13. What security measures does the utility take to ensure that customer information is delivered securely from the meter to the utility?

A.

The smart meter encryption mechanism protects the data as it travels through the mesh network all the way back to the FPL back office systems. Along the way, the data is aggregated at the access points for transmission to the FPL back office systems via public cellular carriers and is protected with additional data encryption.

In addition, It is important to emphasize that FPL smart meters do not store or transmit any personally identifying information.

Q.

14. How does the utility ensure that smart meters are protected from cyber hacking?

A.

It is important to emphasize that FPL smart meters do not store or transmit any personally identifying information.

Over the past several years, FPL has engaged multiple third-party cyber security experts to conduct analysis and testing of various parts of the smart meter solution; from the smart meter to the back office systems. These testing efforts involved a variety of architectural and threat analyses, hardware and software penetration testing as well as automated and manual code reviews. There has been validation that the usage information transmitted from an FPL smart meter is encrypted and that the various components along the data path are secure. Additionally, the current industry standard for the security of the smart grid is documented within the NISTIR 7628 guideline from NIST and FPL is in compliance with this standard.

FPL's Information Security group has been involved with the design and development of the Energy Smart Florida (ESF) program since its inception and has a thorough Cyber Security Plan approved by the DOE for this program. The philosophy has been to ensure that security drives the development of the smart meter solution and that security is factored in at every possible opportunity.

FPL has been actively involved not only with its principal smart meter vendors, but has also built partnerships with other utility industry members across the country who are also deploying smart meters. This Security Consortium, of which FPL was a co-founder and the former chairman, meets quarterly to discuss smart meter security issues and share information in an effort to influence the direction of the smart meter vendor's security roadmap to address evolving industry standards and emerging security concerns.

Q.

15. What are the cost components of metering service currently included in customer rates?

A.

The significant components of metering services included in Customer Rates today are the cost of meters, along with the operational costs associated with meter reading and field services. These include the following;

- Physical meters and infrastructure (capital)
- Meter reading operational costs (meter readers, vehicles, supervision, routing)
- Telecommunications expense for backhaul (communication cost for Smart Meters)
- Customer communications (notification that meters will be installed)
- Meter can repairs associated with Smart Meter installations
- Meter testing and associated technologies at FPL's Meter Technology Center
- Disconnect/reconnect meter for non-payment (field collectors, meter men, vehicles, supervision, equipment)
- Field meters expense for move in/move out changes and maintenance of meters (meter men, vehicles, supervision, equipment)
- Revenue Protection – activities associated with identifying theft of electricity (meter men, vehicles, supervision, equipment)

Q.

16. Under what circumstances should an alternative to a smart meter be offered?

A.

As we have previously described, there are no technical reasons why smart meters should not be installed; smart meters are the most cost effective metering solution and offer the greatest benefits to our customers. However, if the Commission implemented a program in which FPL would be authorized to recover all costs associated with maintaining an alternative meter, this alternative could be made available to customers who request it or refuse access to their property.

It would be unfair to ask all customers to subsidize the costs incurred as a result of other customers' decisions. This is consistent with other customer choice alternatives such as underground service for which all incremental costs are charged to the customer requesting the non-standard alternative.

Q.
17. If an alternative to a smart meter were to be offered, what are the costs of providing that service?

A.

We know that there are many systems, processes and staffing requirements that would be affected by requiring an alternative to the standard smart meter. Some of these are:

- major modifications to the customer information system to properly track and process accounts for these customers,
- enrollment processes through our Care Center, Web Portal and Voice Response System,
- field visits for physical meter reading,
- special billing and collections processes,
- special meter testing,
- special outage identification and restoration processes,
- additional network devices to fill gaps created by non-communicating alternative meters
- installation of smart meter for next customer, and
- field visits for meter connect/disconnects.

The total number of customers who are willing to pay for an alternative meter, and where they are located, will have a significant impact on the costs to provide this service. Although right now we can't accurately determine the cost impact until we know all these variables, based on our current estimates, the incremental costs for an alternative meter could exceed $1,000 per customer over a five year period. The costs per customer will likely change over time depending upon participation rates and accordingly should have a periodic re-evaluation mechanism.

Q.

18. How should the rate for that service be calculated?

A.

All incremental capital and operating expenses incurred for providing an alternative meter should be charged to the customers requesting an alternative meter through an initial upfront charge and a monthly recurring charge. These charges should be reviewed periodically and revised for current costs and participation rate.

Q.

19. How does an opt-out affect the cost-effectiveness of the utility's current smart meter roll-out?

A.

As we have previously described, smart meters are the most cost effective metering solution and offer the greatest benefits to our customers. Permitting customers to opt out will have a negative effect on the savings and operational efficiencies of the smart meter program, requiring us to maintain many redundant systems and processes for meter reading, collection, and meter maintenance services.

We would not be able to accurately determine what the initial impact would be until the smart meter deployment is complete.

Q.

20. What is the feasibility of using a wired option over wireless transmission of customer metering data? What is the cost difference between the technologies?

A.

FPL utilizes a wide variety of communication technologies in the various parts of our business including fiber optics, dedicated wire-based phone lines, satellite, Ethernet, and wireless communication technologies. In choosing the best communication technology for smart meters, FPL did a comprehensive assessment which included a two year smart meter pilot before selecting the wireless technology we are deploying. Fiber optics and wire-based telephone line connectivity to the home are not feasible options due to the prohibitive cost of the required communications infrastructure and lengthy construction time. High-level estimates to provide wire-based smart meter connectivity to 4.6 million customer premises is approximately $5-$6 billion for fiber optics and $225-$250 million for activating dedicated phone lines along with an estimated $100-$125 million/month in phone charges. Both wire-based options would cost over ten times that of a wireless option and add many extra years to the project schedule.

The two year FPL smart meter pilot included both wireless and wired technologies. At the pilot conclusion, FPL used the pilot results along with results of a comprehensive technology evaluation for the short and long term requirements of the smart meter network to determine the most appropriate and effective smart meter communications technology. The wireless technology design was selected over all other options because it required substantially less infrastructure to deploy, lowering the costs compared to any wire-based technology. It also provides the required bandwidth, scalability, and reliability for FPL's smart meter program and compatibility with our smart grid applications. Wireless technology remains the predominant industry choice for today's smart meter deployments.