National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW.
Room 4725
Attn: IOT REC 2016
Washington, DC 20230

Re: Docket No. 160331306-6306-01—Response of the Edison Electric Institute to the IOT Request for Public Comment

Ladies and Gentlemen:

The Edison Electric Institute ("EEI") on behalf of its member electric utilities submits these comments in response to the National Telecommunications and Information Administration's ("NTIA") Notice of Request for Public Comment ("Notice") published on April 6, 2016 regarding "The Benefits, Challenges and Potential Roles for the Government in Fostering the Advancement of the Internet of Things."[1] In particular EEI will address Question 6 (a)(iii) concerning how the lack of adequate spectrum and potential congestion and interference could hinder the development of the Internet of things ("IoT"), Question 6 (b) the steps that the government might take to mitigate the issue and the benefits of government/private sector partnerships, and Question 16 the government role in responding to cybersecurity concerns.

EEI is an association of United States investor-owned electric utilities and industry associates worldwide. Its U.S. members serve almost 95 percent of all customers served by the shareholder-owned segment of the U.S. industry, about 70 percent of all electricity customers, and generate about 70 percent of the electricity delivered in the U.S. EEI frequently represents

[1]National Telecommunications and Information Administration, *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, Notice of Request for Public Comment, 81 Fed. Reg. 19956 (published April 6, 2016).

its U.S. members before Federal agencies, courts and Congress in matters of common concern, and has filed comments in various proceedings affecting the interests of its members.

Electric utilities are critical infrastructure industry ("CII") entities which rely heavily on communications for critical monitoring and control of this nation's transmission and distribution grid, emergency and other communications, smart meters/AMI, *etc*. At present, the electric industry is beginning to undergo a transformation as result of the introduction of new technologies, new clean sources of power, and changing needs and expectations of customers. In order to meet new demands, the industry has invested billions of dollars in modernizing this nation's grid by deploying the Integrated Grid[2] which is more popularly known as the Smart Grid[3]. Grid modernization is critical to maintaining the resiliency, reliability and security of the grid as well as "achieving national goals of energy in dependence and efficiency."[4] The Smart Grid represents the convergence and application of electric, telecommunications and IoT technologies. Having access to adequate spectrum and addressing cybersecurity concerns are critical to the deployment of the Smart Grid.

Consequently, EEI and its members are particularly interested in this proceeding and how national IoT policies may impact—either positively or negatively—grid modernization. The electric industry is concerned that the lack of adequate spectrum, potential congestion and interference, and inadequate attention to cybersecurity risk by IoT technology developers will impede the deployment of the Smart Grid and could negatively affect the reliability, resiliency

[2] *See e.g.* Electric Power Research Institute *The Integrated Grid Realizing the Full Value of Central and Distributed Energy Resources* (2014)
[3] The term "Smart Grid" is a misnomer because not only is this nation's grid already smart it is one of, if not, the most advanced energy systems in the world.
[4] Federal Communications Commission *The National Broadband Plan* at 247 (2010)

and security of the grid as well as impede progress towards achieving national goals regarding clean power and energy efficiency.

I. Question 6 (a)(iii)—Potential Harm Caused by the Lack of Adequate Spectrum and Congestion and Interference

A. The Integrated Grid (AKA Smart Grid) is Critical to This Nation's Future

Energy has become even more vital to our nation's continued economic growth and security. Today's electric power industry facilitates all of America's public safety, business and trade, infrastructure, education, health, social interactions and political and cultural life. Any outage, regardless of extent and duration, has immediate societal and economic impacts (*e.g.*, government and industry closures that would curtail the provision of critical services and employment, as well as emergency and critical services such as public safety, hospitals services, and gasoline supplies). Quantum leaps in demand for broadband telecommunications capacity and computing power have translated into a sustained demand for even more abundant and reliable power supplies. Moreover, without access to energy few, if any, IoT applications would work. With so much riding on them, electric utilities have risen to the challenge by striving to become even more resilient, secure and reliable in the face of natural disasters and potential security threats.

In order to provide resilient, reliable and secure service, as well as to accommodate new sources of power such as wind and solar, EEI's members make extensive use of communications both as owners and operators of private communications systems, and as end-users of commercial communications networks. Electric utilities utilize both licensed and unlicensed spectrum. They are in fact among this nation's largest users of communications networks and services. Electric utilities make particular use of wireless communications in their vital

supervisory control and data acquisition ("SCADA"), distributed automation and field operations systems.

Electric utilities are now investing billions of dollars in communications plant as part of the effort to digitize the grid and to deploy the Smart Grid. Although there is no one definition of the Integrated Grid or Smart Grid, it is generally understood to enable the two-way flow of electricity and information to create an automated, widely distributed energy delivery network by combining electric, telecommunications and IoT technologies. It has tremendous capabilities including integrated two-way communications, advanced components, advanced control methods, sensing, monitoring and measurement, and improved interfaces and decision support. According to an Electric Power Research Institute study, grid modernization through the deployment of Smart Grid technology will result in benefits such as improved reliability, improved utilization of alternative energy sources, improved ability to detect and respond to physical and cyber attacks, distributed technologies and innovation, as well as empowering consumers to make informed choices.

In 2010 in its report entitled "Communications Requirements of Smart Grid Technologies" the Department of Energy ("DOE") stated that the evolution toward a Smart Grid was a major technological change of national scope and "communications technologies are one of the critical foundations of this change."[5] DOE recognized that the communications requirements of the Smart Grid would fundamentally change how the electricity network employs communications technologies.[6] Moreover, because it relied on the increased use of communications and information technology, sufficient access to communications facilities was

[5] Department of Energy *Communications Requirements of Smart Grid Technologies* at 5 (2010).
[6] *Id*.

critically important. DOE also recognized that wireless technologies could offer advantages over other technologies for certain Smart Grid applications and deployments as they related to data applications.[7]

In the report entitled Field Area Networks the authors discussed the importance of Communications to the Integrated Grid and how it facilitated the use of various related IoT applications.

> Modernization of utilities and other critical infrastructure industries (CII) has made it clear that communications networks are critical to maintaining the safe, reliable and efficient delivery of essential electric, gas and water services to the public at large. Grid modernization is already requiring that communications networks meet an increasingly rigorous set of requirements designed to support new and more time-constrained and critical applications. Today's electric utilities have deployed communications based upon applications that provide network operators with the capability to monitor grid problems in real time, and teleprotection programs that require as few as 20 milliseconds round trip latency in order to respond to and prevent faults from cascading into major outages. The evolving role of utilities in the integration of distributed energy resources is placing even greater demands on their communication networks, to balance inconsistent solar and wind energy resources with uncertain demand and storage resources, such as water heaters and variable speed air-conditioning compressors. The utility's role in keeping supply and demand in balance at the edge of the grid will enable the optimization of the use of existing resources, while avoiding (or at least delaying) the need for new generation and/or distribution infrastructure upgrades. Such advances require continuous evolution in utility communications networks.[8]

B. Dedicated RF Spectrum is Needed to Power New Energy and Communications Technologies

Utilities have come to rely on RF wireless spectrum for critical and emergency communications. With regard to the future, RF Spectrum will play a critical role in all utilities pioneering ground-breaking energy and communications technologies, including facilitating and enabling the rapidly developing IoT. Utilities need RF spectrum to monitor and control millions of devices. As overall energy demand accelerates and variable generation proliferates, utilities

[7] *Id*. At 51
[8] Smart Networks Council/Edison Electric Institute *Field Area Networks* at 1 (2015).

will need dedicated RF spectrum for broadband communications to manage peak loads, to maintain grid stability and to support communications networks to monitor and control millions of devices and the new generation resources that will be connected to utility systems.

Wireless communications is important for reliable electric utility operations because it is a propagating medium which cannot be destroyed or damaged by a natural or man-made disaster. As CII entities, utilities cannot rely upon commercial networks to meet their needs for reliability and resiliency with regard to critical communications because commercial networks are not sufficiently reliable or resilient. While utilities have extensive wireless communications networks, they use narrowband frequencies, which may not support the increasing capacity requirements that have been created by the deployment of the Smart Grid and grid modernization. Without guaranteed access to suitable RF spectrum, America's electric utilities will not have the tools they need to modernize, much less maintain, their networks' security, resiliency and reliability.

II. Question 6 (b)—Steps That The Government Might Take To Mitigate The Issue

Utilities need access to 10 megahertz of spectrum that is suitable to support different communications needs, including voice and data, in different environments, including rural and urban areas. To provide the necessary coverage, this spectrum will need to be in a single band or two separate bands with sufficient propagation and bandwidth to provide sufficient capacity and coverage to enable the development and deployment of a cost-effective, highly-reliable, wide-area, high-capacity wireless infrastructure.

Utilities must be permitted by the FCC or NTIA to enter into Licensed Shared Access (LSA) agreements (i.e., as "priority access" users) with either commercial mobile providers or

with Federal incumbents in some bands–potentially in the 5 GHz bands now under consideration for Wi-Fi reallocation domestically and internationally. Licensed Shared Access or Authorized Shared Access of the 406-420 MHz band and the 4.9 GHz public safety spectrum are viable options should also be permitted. Such a government/private sector partnership would be very beneficial and in the public interest.

III. Question 15—The Government Role in Addressing Cybersecurity Concerns

Electric utilities are consumers of information and communication technologies (e.g., IoT)—both for business and operational systems. Utility concerns are similar to other consumer concerns regarding cybersecurity, except that cybersecurity risk is carefully considered in utility procurements and operations. Other CII entities are likely similarly focused on cybersecurity risk, whereas individual consumers may not prioritize security in their purchasing decisions. Also, cybersecurity of the most critical grid systems is regulated by the Federal Energy Regulatory Commission (FERC). Cybersecurity risk and regulation are key drivers into how and whether utilities will adopt IoT technologies. The challenges utilities face as consumers of IoT technologies is that they cannot control the cybersecurity vulnerabilities introduced during the development of the technologies. Utilities can only mitigate the risks within their operational boundaries, especially during integration and operations, although utilities can negotiate with their suppliers during procurements or acquisition of IoT technologies. The early parts of the supply chain—development, design, and manufacturing is the responsibility of the supplier or IoT manufacturer.

Unfortunately for consumers that prioritize security, innovation often first focuses on developing a technology that provides a new feature or convenience to a consumer that will

attract a market. Cybersecurity is often not addressed until the market starts to mature and consumers ask for security. To help drive innovation of IoT while balancing cybersecurity risk for all consumers—not just utilities—the government may want to consider developing easy to follow policies or standards for IoT manufacturers regarding software development best practices. Existing practices already exist, so the challenge will be in getting IoT innovators to use these practices, especially if they are new companies with less resources to focus on secure software development. This presents a good role for the Department of Commerce and the federal government—to help innovators address security.

A possible approach to be considered in addressing cybersecurity is to tie grant and other IoT funding to security requirements. For example, DOE required their Smart Grid Recovery Act Programs to address cybersecurity in their grant projects and DOE worked with the National Institute of Standards and Technology and other standards development organizations to develop tools, standards and best practices.[9] Although integrating cybersecurity requirements into innovation grants is a good start, security is an ongoing challenge, and risk management must continue after grant funding is spent. Therefore programs that periodically test new and existing IoT technologies would be useful to consumers to ensure that manufacturers are addressing cybersecurity in their products. Testing manufacturing practices is also important to addressing cybersecurity risk for IoT technologies. In considering these programs, we recommend that the government try to leverage existing programs as well as consider that some manufacturers may also have their own capabilities to verify the security of their products. Outreach to consumers may also be effective in helping to ensure that both manufacturers and consumers are thinking about cybersecurity as they develop and use IoT technologies. Finally, as NTIA is reviewing

[9] *See* SmartGrid.gov, available at: https://www.smartgrid.gov/recovery_act/overview/standards_interoperability_and_cyber_security.html

questions of security and interoperability, electric utilities must be part of those conversations to share lessons learned as well as requirements (e.g., security and regulatory) for them to adopt IoT technologies.

Respectfully submitted,

EDISON ELECTRIC INSTITUTE
/s/ David K. Owens /
David K. Owens
Executive Vice President

Bradford S. Nixon
Associate General Counsel,
Corporate and Regulatory Affairs
Office of the General Counsel

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

H. Russell Frisby, Jr.
Jonathan P. Trotta
Counsel
STINSON LEONARD STREET LLP
1775 Pennsylvania Ave, NW
Suite 800
Washington D.C. 20006
(202) 785-9100
(202) 785-9163 (Fax)
russell.frisby@stinson.com
jon.trotta@stinson.com

Dated: October 26, 2015