VIA Email to iotrfc2016@ntia.doc.gov

June 1, 2016

National Telecommunication and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Washington, DC 20230

ATTN: IOT RFC 2016

RE: The benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

Comments Submitted on behalf of the IEEE-USA

Thank you for giving the IEEE-USA this opportunity to comment on the NTIA's role in promoting and regulating the Internet of Things (IoT). IEEE-USA is the American component of the IEEE, representing the 200,000 IEEE members who reside in the United States.

As the Department of Commerce (DOC) and Administration have long recognized, the IoT has tremendous potential to change how Americans work and live. Technological innovation is allowing IoT technology to revolutionize health care, energy production and distribution, personal security and, frankly, just about every other part of society, making this an enormously exciting time to be a technology professional.

But while the promise of the IoT is obvious, so are the risks. Ubiquitous interconnectivity is creating new vulnerabilities in our society to cyber-attacks and cyber-crimes. These risks can put people's finances, privacy and even lives in danger if not properly mitigated. The IoT also presents the United States with infrastructure challenges, as new technology and applications require faster internet connections, and more wireless spectrum.

These risks will require an active and enlightened response from the federal government.

In general, the federal government's role should be ensuring that the IoT serves the public interest. Fulfilling that role must include insisting that the legal and regulatory structures governing the IoT are developed in an open process and that this process incorporates voices from all affected stakeholders, especially technology experts.

Most of all, the government must build governance systems that are flexible and technology-neutral. Products, companies and entire lines of technology will be created, and destroyed, in the coming years. America's regulatory agencies must be ready to respond to these changes, and adapt when necessary.

The IEEE-USA, along with the IEEE Internet Initiative, recommend the following more specific ways the federal government can help nurture and promote the IoT.

Defining the Internet of Things:

"Internet of Things" is a general term used to describe technology that can communicate remotely with other technology using systems that are independent of either technology. The IoT also encompasses the enabling systems that allow this communication to occur. That is a very broad definition. It is also very vague, since there is no commonly agreed upon limits to what is included in the IoT. As a result of its broadness and vagueness, "Internet of Things" encompasses a huge number of widely diverse technologies.

But this does not mean the definition is bad. "IoT" is a useful term. The unifying characteristic of "connectivity" is sufficiently specific to be meaningful, and also points to the source of the technologies' promise and challenges. Moreover, nobody – not the government, industry or academia - knows what, exactly, the IoT will become. Innovative technology is being developed across our economy that puts internet communications to work in surprising ways every day. It would be unwise it narrow the definition of the IoT before anyone really knows what the IoT will become.

We suggest that it would be useful for the Department of Commerce to keep the broad and vague term "IoT" in use, but then subdivide the topic into technology-specific sectors, such as transportation, personal communication, sensors, etc. It will be easier to both define and deal with these subsets than the entire IoT since members of the subsets will have much more in common. The more specific subsets will also pose similar policy challenges, and therefore can be dealt with more easily by the government.

NIST ought to be given responsibility for developing and defining these sub-groups, with assistance from industry, professional associations and other stakeholders. While doing so, NIST should always keep in mind that their definitions need to allow for the development of technology that has not yet been imagined, and that therefore won't fit into clearly defined categories. In fact, the most important innovations probably won't.

Spectrum Needs:

As wi-fi technology continues to improve, more and more technology will use wireless communication protocols to communicate (although not all IoT technologies will do so). This will increase demands on already scarce wireless spectrum. Moreover, emerging technologies will likely use existing spectrum in new, innovative and perhaps disruptive ways. The FCC in particular will need to find ways to make more spectrum available for IoT technologies, and be as flexible as possible when permitting the use of that spectrum.

Stakeholder Coordination:

The federal government can play a useful role improving communication between industry, academia, professional societies and the general public. The IoT will require coordination across all stakeholders to identify and assess technology gaps, establish security protocols, address issues related to privacy and civil liberties, and discuss the trajectory of technology innovation. Such coordination will help the marketplace respond faster to changing technology, and help, for example, academia keep up with changing labor market needs. The promise of the IoT is in its ability to tie very different pieces of technology together seamlessly. This requires constant on-going communication between actors in different places and fields. The government, and especially the DOC, is uniquely qualified to lead efforts to meet this need.

Standards:

The foundation of the IoT is connectivity. The products that make up the IoT must be able to communicate with products produced by other companies, based on other technologies, with other purposes. And this communication must be seamless, user-friendly, secure, and in many cases instantaneous.

Conquering these technical challenges will be easier with a library of standards underpinning the entire network.

Fortunately, the technology community has already proven that it is capable of developing global industry standards that promote innovation, competition and the public good. Wi-Fi (IEEE 802.11), for example, has been very successful at establishing a global web of technologies that can operate together flawlessly.

NIST, the EPA and other government agencies have similarly shown that the federal government has an important role to play in promoting the use of standards, while not developing the standards themselves. Government agencies, by partnering with Standards Development Organizations (SDOs), can promote the development of standards, support the development process, and help bring together relevant stakeholders. It is important that the actual standards be developed by the private sector, which will have a much better understanding of the directions technology is moving and what is technically possible. But the DOC, among other Departments, needs to play a leadership role helping standards efforts to get organized, and then supporting these efforts.

Public Trust – Protection, Security, Privacy and Safety:

It will be essential, if the IoT is to reach its potential, that the networks and devices enabling the IoT be secure, private, and safe. Some of this can be accomplished through security standards, which can be negotiated (with government help) through SDOs. But much cannot. Questions about privacy for people using the IoT are policy, not engineering, concerns. As such, the fundamental questions about how secure, private and safe a network must be should be answered in a more public forum. In some cases this will require new laws, but in others the DOC could play an enormously useful role in promoting the IoT by using the rulemaking process to establish norms and expectations.

Privacy, safety and security are intrinsically important. But more than that, the public will not use the IoT if they don't trust it. Good rules are needed to ensure that the public feels comfortable using computer networks to handle their personal finances, medical information, shopping, and hundreds of other things. Good rules are also necessary to ensure that people will be comfortable using IoT devices in their homes, entrust the safety of their loved ones to IoT-connected transportation, and support funding of IoT-connected infrastructure. This is why the public, through its elected government, needs to be given an explicit, and central, role in developing the IoT rules on privacy, security and safety, and why this process must be transparent. People are more likely to trust systems they help design, and that will require a Department-led effort.

International:

To reach its full potential, the IoT should be as global a network as possible. The NTIA, along with other parts of the federal government, has an important role to play representing the United States at

international organizations such as the ITU and WIPO. These institutions play a vital, if often un-noticed, role in building and regulating the structures that support IoT technologies. Naming conventions and registration of "named" elements may not be well understood by the public, but they must be done well for the IoT to flourish.

The NTIA and other involved government agencies need to ensure that this backend governance of the IoT, and internet more broadly, be open, transparent, responsive and flexible. Individuals and companies involved in developing new IoT technologies need to both understand and have a means to change the rules that give the IoT structure. Working through low-profile international organizations is difficult for smaller stakeholders. The NTIA should aggressively reach out to these stakeholders to make sure their concerns are heard.

The IEEE-USA represents 200,000 individual engineering, computing and allied professionals in the United States, and is part of the IEEE which represents over 436,000 of these individuals world-wide. These comments do not necessarily reflect the views of IEEE nor any of its other operational units.