Open Connectivity Foundation
3855 SW 153rd Drive
Beaverton, OR 97003
Email: staff@openconnectivity.org

To:

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

Mr. Lawrence E. Strickling,
Assistant Secretary for Communications and Information

I am writing in response to RIN 0660-XC024, request for public comment on "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things". Thank you for the opportunity to comment on the important issues raised in the document. In this response I provide some background information on the Open Connectivity Foundation (OCF) before replying to several of the specific questions raised in your request. We anticipate and look forward to continued work with the Department of Commerce on these topics in the future.

Yours sincerely,

Michael S. Richmond
Executive Director
Open Connectivity Foundation

Open Connectivity Foundation

The Open Connectivity Foundation (OCF – http://www.openconnectivity.org) is a non-profit alliance of companies – currently over 180 and growing rapidly – including industry leaders such as Arris, Cablelabs, Cisco, Electrolux, GE Digital, Intel, Qualcomm, Microsoft and Samsung. The current member list can be found at http://openconnectivity.org/about/membership-list.

The organization's goal is to enable a vibrant IoT ecosystem by delivering a standardized communications framework for the Internet of Things and a standardized data model via which applications and services may interact with it. OCF develops an open specification and related certification program, plus predictable IP protection & branding for certified devices (via compliance testing). OCF also sponsors the open source IoTivity (https://www.iotivity.org) project, which is run by the Linux Foundation and develops a reference implementation of the OCF specification.

OCF technology is designed to service multiple vertical markets, in part because there are many common problems across the markets, but also because important use cases require interoperability across vertical markets.

Responses to Specific Questions

OCF does not have a view on all the questions raised in RIN 0660-XC024, but wishes to answer the following:

> *1. Are the challenges and opportunities arising from IoT similar to those that governments and societies have previously addressed with existing technologies, or are they different, and if so, how?*

The challenges are similar to the development of the Internet and the standardized applications (e.g. the World Wide Web, e-mail, and many more) that utilize it. There are, however, three important differences:

1. IoT will involve orders of magnitude more devices providing vast quantities of data and control points.
2. Client-server (device-to-Cloud) and server-server (Cloud-to-Cloud) communications models that are familiar from the Internet will continue to be important. However, a much higher percentage of communications will be between devices that are currently regarded as clients: device-to-device, device-to-gateway, and gateway-to-gateway.
3. A much higher percentage of interactions between devices will be autonomous.

> *1.a. What are the novel technological challenges presented by IoT relative to existing technological infrastructure and devices, if any? What makes them novel?*

OCF is mainly concerned with a specific but far reaching IoT challenge. The value of IoT will be delivered by applications and services that access the new data and control points, but reaching the necessary scale requires three things:

1. Easy data interoperability, across devices, platforms, operating systems, manufacturers and vertical markets.
2. Enabling a majority of software developers to build IoT applications and services, most of who come from a background of web-service, or app development and have limited familiarity with embedded programming and lower-layer communications protocols.
3. Security of data and control points so that only authorized applications and services have access.

These requirements drive the need for the standardized data models and communications framework that OCF is designed to deliver.

> 1.c. What are the most significant new opportunities and/or benefits created by IoT, be they technological, policy, or economic?

We believe there will be significant new benefits and or opportunities in all three areas: technology, policy and economic. IoT will connect things to things and things to people in a way that has never happened previously. This level of interconnectedness will drive a wave of new business ideas and economic growth greater than the growth resulting from the creation of the internet. This will require innovation in technology to meet the demands of interconnectedness and new ways to approach policy definition as IOT will move very quickly and work horizontally across vertical market segments previously unrelated.

> 2. The term ''Internet of Things'' and related concepts have been defined by multiple organizations, including parts of the U.S. Government such as NIST and the FTC, through policy briefs and reference architectures. What definition(s) should we use in examining the IoT landscape and why? What is at stake in the differences between definitions of IoT? What are the strengths and limitations, if any, associated with these definitions?

The Internet of Things can be broadly understood as the result of compute and communications capabilities lowering in cost (and size, and power) to the point where they can enable devices that would otherwise be "dumb and isolated" to be "smart and connected". The implications of this extends far beyond the devices themselves into the entire data and communications ecosystem. It is – in a term popularized by Cisco – the Internet of Everything. It is therefore impossible to use just one set of definitions or a single architecture to understand all of IoT.

OCF recommends that one of several approaches used when conceptualizing IoT is the need for end-to-end interoperability between services, applications and devices. The OSI 7

Layers model of communications is useful in the context. OCF's approach is to standardize at a high "data model" layer and provide translations from this standard down onto a variety of lower layers – including different MAC/PHYs – and across to other data models used by non-OCF devices. In this way it provides a high level of interoperability across currently fragmented ecosystems as well as a path towards eventual consolidation.

The U.S. Government should consider all layers of the IoT communications model when making any decisions to ensure that recommendations or legislation affection one layer don't have unintended consequences on other layers.

> 4. Are there ways to divide or classify the IoT landscape to improve the precision with which public policy issues are discussed? If so, what are they, and what are the benefits or limitations of using such classifications? Examples of possible classifications of IoT could include: Consumer vs. industrial; public vs. private; device-to-device vs. human interfacing.

While different vertical segments of IoT may have differing needs, and considering them separately may be useful in some respects, it is important to also consider what requirements and technologies are and should be common across multiple segments. A combination of the two approaches is necessary.

If commonalities are not considered the result will be inefficiencies – different segments duplicating effort – and eventual barriers to implementing more complex usages that require interoperability across segments.

OCF believes that interoperability at the data model level is a feature that should be common across segments.

> 6. What technological issues may hinder the development of IoT, if any?
> a. Examples of possible technical issues could include:
> ii. Insufficient/contradictory/proprietary standards/platforms

Given the scope of IoT it is inevitable that there will be different standards and platforms, particularly during the early stages of IoT development. The ability to provide interoperability via translation between standards will therefore be key. Ultimately the entire IoT ecosystem will benefit if there is eventual consolidation around open standards.

OCF provides one such open standard, which is also designed to act as a common translation layer between non-OCF devices and protocols.

> 6.b. What can the government do, if anything, to help mitigate these technical issues? Where may government/private sector partnership be beneficial?

OCF believes the best way to promote consolidation around open standards is via voluntary, industry-led, open participation in OCF and similar organizations. The

government can help mitigate technical issues by funding research that supports and employs open standards, and choosing products and services that are based on them.

> 7. NIST and NTIA are actively working to develop and understand many of the technical underpinnings for IoT technologies and their applications. What factors should the Department of Commerce and, more generally, the federal government consider when prioritizing their technical activities with regard to IoT and its applications, and why?

The Department of Commerce should prioritize its efforts on the issues that most concern consumers – security and privacy, and the issues that most concern industry – openness and the encouragement of innovation.

> 8. How will IoT place demands on existing infrastructure architectures, business models, or stability?

Poorly thought-through architectures will needlessly increase the load on backbone architectures of the internet.

> 9. Are there ways to prepare for or minimize IoT disruptions in these infrastructures? How are these infrastructures planning and evolving to meet the demands of IoT?

As much as possible, the stewards of the internet and the web are trying to guide IoT standardization toward adaptation of existing protocols vs, completely new protocols.

> 15. What are the main policy issues that affect or are affected by IoT? How should the government address or respond to these issues?

In traditional computing, the end user initiates and interaction. Automatic initiation is not unknown in today's environment, but it will predominate in the era of IoT. Consumer awareness and notification should be a key government concern.

Given the complexity, size and speed at which we anticipate IoT to evolve, it is not yet possible to predict all areas where policy issues may arise. One potential issue will be reacting quickly enough with policy changes. Government support of open, voluntary, industry-led collaborative initiatives like OCF and their ability to address issues quickly is one approach to help minimize this issue.

> 16. How should the government address or respond to cybersecurity concerns about IoT?
> a. What are the cybersecurity concerns raised specifically by IoT? How are they different from other cybersecurity concerns?

IoT has the potential to unlock tremendous socio-economic value by connecting devices and sharing data. This level of interconnectedness will generate data on an entirely new

scale. Securing data and devices while ensuring privacy are two concerns. Organizations like OCF are aware of the importance of security and privacy and are working to implement architectures that protect data, devices and privacy while being flexible to adjust to future threats. This can only be achieved by open and collaborative approach to cybersecurity

> 16.c. What role or actions should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to IoT cybersecurity, if any?

The Department of commerce should support open industry, collaborative efforts already underway to address cybersecurity in organizations like OCF and other open, standard efforts.

> 17. How should the government address or respond to privacy concerns about IoT?
> a. What are the privacy concerns raised specifically by IoT? How are they different from other privacy concerns?

The answer to question 16.a. above applies equally to privacy as to security. The two are intimately related.

> 17.b. Do these concerns change based on the categorization of IoT applications (e.g., based on categories for Question 4, or consumer vs. industrial)?

We do anticipate there will be unique privacy concerns based on the applications outlined above in question 4.

> 17.c. What role or actions should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to privacy and the IoT?

The Department of commerce and the federal government in general should support and engage with open, collaborative efforts already underway to address privacy in organizations like OCF. Support and engagement will result in solutions that meet the need of consumers and business while insuring the government has clear visibility and can monitor what is happening and providing guidance where concerns may arise.