CompTIA.

June 2, 2016

National Telecommunications and Information Administration

U.S. Department of Commerce

1401 Constitution Avenue NW.

Room 4725

Attn: IoT RFC 2016, Washington, DC 20230

To Whom It May Concern:

The Computing Technology Industry Association "CompTIA" respectively submits our comments on the NTIA Internet of Things Request for Comments. According to CompTIA's *Sizing Up the Internet of Things* (IoT) report, the Internet of Things will be composed of 50.1 billion connected devices by the year 2020 and $1.9 trillion in global economic value-add. These devices, driven by "smart" sensors (pushing data into the cloud to be analyzed), hold the promise of connecting communities and businesses, helping deliver smarter services to the American public while revolutionizing business sectors. As a country, it is critically important that we have a balanced approach to IoT, one that recognizes the voices of all the stakeholders in the IoT ecosystem.

David Logsdon

Senior Director, Public Advocacy

CompTIA

CompTIA

CompTIA Submission for the NTIA IOT Request for Comments

General:

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 difference is based on the immense number of stakeholders involved in IoT. Each stakeholder brings unique capabilities to the marketplace which brings its own set of challenges and opportunities.**

a. What are the novel technological challenges presented by IoT relative to existing technological infrastructure and devices, if any? What makes them novel? **To date, most sensored based communication has been siloed. What makes IoT potentially unique is the ability of sensors to communicate across a wide variety of verticals.**

b. What are the novel policy challenges presented by IoT relative to existing technology policy issues, if any? Why are they novel? Can existing policies and policy approaches address these new challenges, and if not, why? **The existing policies and policy approaches are good placeholders for now. We must get a better understanding of the IoT ecosystem and ensure that collectively those stakeholders enhance the policies and policy approaches.**

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

By making things connected that otherwise would not be, IoT drives the potential for efficient economies and citizen facing services. IoT is about connecting the urban to the rural and vice versa. The phenomena of IoT will help accelerate city leadership to identify current technological capabilities and potential gaps. The analysis will also help identify areas where are needs for workforce training and certification.

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.

8 What definition(s) should we use in examining the IoT landscape and why? **An ecosystem of connected devices that enables the unsiloing and smartification of communication. IoT drives the potential for efficient economies and citizen facing services.** What is at stake in the differences between definitions of IoT? What are the strengths and limitations, if any, associated with these definitions?

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. **Consumer vs. Industrial with the realization that the classifications will have cross cutting issues.**

6. What technological issues may hinder the development of IoT, if any?

a. Examples of possible technical issues could include:

i. Interoperability

ii. Insufficient/contradictory/proprietary standards/platforms

iii. Spectrum availability and potential congestion/interference

As the Internet of Things continues to grow in the coming years, the demand for more wireless spectrum to carry the transmissions from these billions, if not trillions, of devices, will grow as well. Demand for more spectrum isn't just coming from IoT devices, however, but from increased wireless traffic as well. To prepare for this increased demand, the government must make as much spectrum as possible available for both licensed and unlicensed use without technology-specific restrictions on its use.

According to projections from both Cisco and Ericcson, mobile and IoT traffic will continue to grow by leaps and bounds in the coming years. Cisco projects that mobile data usage will increase nearly sevenfold in the U.S. from 2014 to 2019,[1] while Ericcson projects usage in 2019 will be five times that in 2014.[2] Ericcson also projects that there will be more IoT connections than mobile connections worldwide as soon as 2018 and make up 57% of connections by 2021.[3] While some of these IoT connections will use licensed spectrum, Ericcson projects that in 2021, more than 90% of IoT connections will use unlicensed spectrum.[4] However, they also project that licensed spectrum's importance to IoT will start to increase in 2020 and continue to grow as 5G networks are deployed. [5]

This massive increase in both mobile and IoT connections will necessitate a significant increase in the amount of available licensed and unlicensed spectrum available for IoT use. While a number of efforts are underway to increase the amount of available spectrum, such as the FCC's incentive auction and 3.5 GHz proceeding, among others, Congress, the FCC, NTIA, and other federal agencies must continue to work together to make more spectrum available. Passing legislation such as Senator Thune's MOBILE NOW Act (S.2555),[6] which passed the Senate Commerce Committee unanimously in March, would be a great first step, but even more work needs to be done. The federal government remains the largest

[1] Cisco, Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2014-2019, at 36 (Feb. 3, 2015) http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf ("Cisco 2015 Mobile Data Forecast").
[2] Ericsson, North America Ericsson Mobility Report Appendix, at 5 (Nov. 2014), http://www.ericsson.com/res/docs/2014/emr-november2014-regional-appendices-rnam.pdf.
[3] Ericcsson Mobility Report: On the Pulse of the Networked Society, at 10 (June 2016), http://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf.
[4] *Id.*
[5] *Id.* at 11.
[6] MOBILE NOW Act, S.2555, 114th Cong. (2016).

holder of wireless spectrum, and legislation is needed to incentivize agencies to move off of or share their spectrum.

Any new spectrum made available should not be allocated for a specific use, and should instead remain flexible-use spectrum. In such a quickly-evolving industry as IoT, putting technology-specific limitations on bands of spectrum could hinder innovation. Instead, any new spectrum made available should not specifically be dedicated to IoT or mobile use, but should be available for any use. Such a technology-neutral approach will better accommodate new technologies and changing markets.

b. What can the government do, if anything, to help mitigate these technical issues? Where may government/private sector partnership be beneficial? **Most IoT growth will initially be in the urban/city environment. It is important that private industry and city leaders work together to develop a comprehensive understanding of current capabilities and potential gaps.**

8. How will IoT place demands on existing infrastructure architectures, business models, or stability? **IoT, by its very nature, is a digital disruptor. To fully realize the potential benefits of IoT, the infrastructure end user community must ensure the modernization of both the urban and rural infrastructure.**

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? I would reference one of our previous responses. **It is essential that we have ubiquitous, resilient broadband coverage**.

11. Should the government quantify and measure the IoT sector? If so, how? **Government should request that the IoT ecosystem is quantified and measured but leave it up to private industry to do so.**

a. As devices manufactured or sold (in value or volume)? **Yes**

b. As industrial/manufacturing components? **Yes**

c. As part of the digital economy? i. In providing services ii. In the commerce of digital goods **Yes**

d. In enabling more advanced manufacturing and supply chains? **Yes**

e. What other metrics would be useful, if any? What new data collection tools might be necessary, if any? **By the growth in cloud and data service platforms that are directly tied to the IoT ecosystem.**

13. What impact will the proliferation of IoT have on industrial practices, for example, advanced manufacturing, supply chains, or agriculture? **Once IoT is fully ingrained into the industrial practices, end users will be able to measure success by tracking efficiencies.**

b. What will be the challenges, if any? **One of the challenges, in the agriculture community in particular, will be data governance.**

14. What impact (positive or negative) might the growth of IoT have on the U.S. workforce? **Exponential growth in the data analytics, cloud services, and cyber marketplaces.**

16. How should the government address or respond to cybersecurity concerns about IoT?

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? **It is always prudent to consider additional research in regards to IoT security. Therefore, the federal government must consider investing in more research and development funding focused on IoT security.**

17. How should the government address or respond to privacy concerns about IoT?

The growth of the IoT brings with it significant concerns about both consumer privacy and security considering the vast amount of information these newly-connected devices will collect and transmit. However, we believe there are already mechanisms in place to appropriately regulate the industry, and thus we agree with the FTC's conclusion in their 2015 IoT Report that "there is great potential for innovation in this area, and that IoT-specific legislation at this stage would be premature."[7] The IoT is evolving so quickly and unpredictably that any industry-specific legislation could have unintended consequences that hamper the growth of this still-nascent industry.

The FTC has been the chief regulator for privacy and data security for decades, and their approach has been to use their authority under Section 5 of the FTC Act to encourage companies to implement strong privacy and data security practices. This framework is the ideal way to regulate the IOT, as the FTC's technology-neutral case-by-case approach has proven an effective way to ensure companies implement strong data security and privacy protections without stifling innovation. Relying on Section 5's "unfair or deceptive practices" clause and providing guidance through enforcement, the FTC's approach allows it to adjust its enforcement approach as technology evolves and industry best practices change.

Our member companies take privacy and data security protections very seriously, and design their products with these considerations in mind. We agree with the FTC's recommendation that "companies should build security into their devices at the outset, rather than as an afterthought,"[8] by implementing a security by design process. Further,

[7] Federal Trade Commission, Internet of Things: Privacy & Security in a Connected World at vii (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (2015 FTC IoT Report).
[8] *Id.* at 3.

the FTC's 2012 Privacy Report recommended industry best practices for protecting the privacy of consumer data.[9] Companies should follow the FTC's guidance on both security by design and privacy best practices in designing their products to protect their customers' information, or else they could find themselves in violation of Section 5 and bereft of their customers' trust.

In these early stages of the IoT, the only IoT-specific legislation necessary are bills like the DIGIT Act (S.2607) which would convene a working group of stakeholders to make recommendations to Congress on issues such as privacy and security for the IoT. Additionally, we have long-advocated for the passage of a federal data breach notification standard, and we believe the need for such a standard is even more pressing as the IoT grows. Otherwise, industry self-regulation and the FTC's Section 5 authority will sufficiently protect customer privacy and security without the risk of stifling innovation through prescriptive, industry-specific rules.

19. In what ways could IoT affect and be affected by questions of economic equity?

a. In what ways could IoT potentially help disadvantaged communities or groups? Rural communities? **It will be about the effectiveness of citizen facing services, particularly in the urban environment. Each city will have to launch an advocacy campaign to ensure that disadvantaged communities are aware of the citizen facing services available to them. In rural communities, access to IoT services could conceivably launch a new segment of entrepreneurs that bring about the "blue revolution".**

b. In what ways might IoT create obstacles for these communities or groups? **We must make sure, as a nation, that we have ubiquitous broadband coverage so that disadvantaged and rural communities can benefit from the IoT ecosystem.**

d. What role, if any, should the government play in ensuring that the positive impacts of IoT reach all Americans and keep the negatives from disproportionately impacting disadvantaged communities or groups? **In order for our nation to realize the full potential of IoT, we must create a national strategy for broadband (co-lead by a rural based agency and an urban based agency), we must make broadband accessibility a NATIONAL SECURITY PEROGATIVE. Again, it is essential to have uninterrupted, ubiquitous coverage.**

[9] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers at (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (2012 FTC Privacy Report).

Additional Issues:

- **26.** What role should the Department of Commerce play within the federal government in helping to address the challenges and opportunities of IoT? How can the Department of Commerce best collaborate with stakeholders on IoT matters? **The federal government needs a permanent advisory board to help address and advocate for IoT issues. We need to create an IoT Advisory Board- modeled after the National Space Based Position, Navigation, and Timing Advisory Board:**
    - **The National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board provides independent advice to the U.S. government on GPS-related policy, planning, program management, and funding profiles in relation to the current state of national and international satellite navigation services.**
    - **The Advisory Board consists of GPS experts from outside the U.S. government.**
    - **The Advisory Board reports directly to the National Executive Council. The Council is co-led by a civil agency (Transportation) and national security agency (DoD) and represented by the Secretaries from those respective agencies**
    - **Currently, there are 25 members representing U.S. industry, academia, and international organizations**