Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20004

In the Matter of	)	
	)	Docket No. 160331306-6306-01
The Benefits, Challenges, and Potential	)	
Roles for the Government in Fostering the	)	RIN 0660-XC024
Advancement of the Internet of Things	)	
	)	
	)	

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

James Reid, Sr. Vice President, Government Affairs
Avonne Bell, Sr. Manager, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 N. Courthouse Rd
Suite 200
Arlington, VA 22201
(703) 907-7711
abell@tiaonline.org

Submitted electronically via iotrfc2016@ntia.doc.gov

June 2, 2016

EXECUTIVE SUMMARY

The future of telecommunications and the world economy lies with the Internet of Things ("IoT"). IoT is a label for the concept of an increasingly connected future in which regular, everyday items are outfitted with sensors and connected to the Internet to share their data towards the goal of improved data metrics, analytics, and better performance. It holds great potential for positive innovations across all market sectors within the United States and around the world. IoT will give rise to an entire ecosystem for interconnected devices, networks, and data that will enable all users to efficiently utilize a wide range of innovative services and solutions. The IoT model will include a variety of participants in the ecosystem beyond the traditional framework for telecommunications, necessitating policymakers' cognizance of the interests and implications of a much broader set of stakeholders in different sectors and industries.

Network technology and interoperability standards are vital elements of fostering IoT growth. The varied and wide reach of IoT applications are such that it will need to be powered by a host of different technology capabilities targeted as specific functionalities. The technological needs for IoT services targeting "things" in the home or other locations that are stationary and involve short connection ranges will differ significantly from applications that involve regular location change and travel over a longer distance. Additionally, the development of open, voluntary, consensus-based global standards that will pave the way for devices to seamlessly connect to each other and to the network in an interoperable manner is critical.

As a result, policymakers should employ a technology-neutral approach in order to promote the full spectrum of IoT offerings. The U.S. government should adopt policies that incentivize research and development on how to enhance underlying network capabilities and to maximize the use of limited resources such as spectrum. Policymakers should also defer to the multiple efforts in developing global standards that allow for interoperability of IoT technologies because they spur innovation, allow markets and the public to identify the most effective method, and offer a valuable source of scientific and technical information related to the industry.

In addressing IoT policy issues, policymakers should adopt a coordinated, horizontal policy approach whenever possible, followed by tailoring for specific vertical applications. Past policy discussions have developed in a vertical market silos and have overlooked the relation of connected devices to the larger Internet of Things. Horizontal policy issues include encryption for cybersecurity and facilitation of global ICT supply chains. As it relates to cybersecurity, policymakers should avoid heavy-handed regulation that cannot keep pace with the constantly evolving threat and risk landscape and should instead work in public-private partnerships to collaborate on identifying and addressing threats.

The U.S. Government should position its policy efforts in a way that allows consumers and businesses to fully capitalize on IoT's immense potential. In order to fully realize the benefits of the IoT ecosystem, the U.S. Government should adopt policies that: incentivize investment and development of the multiple components of the IoT system; adhere to technology-neutral and competition-neutral principles; and involve collaboration with global partners. All regulatory efforts should attempt to include cross-border coordination and alignment with policies of foreign entities as the marketplace for IoT goods and services will not be cordoned off by geographic or country borders.

I. INTRODUCTION

The Telecommunications Industry Association ("TIA") hereby submits these comments in response to the U.S. Department of Commerce, National Telecommunications and Information Administration's ("NTIA") inquiry seeking public input on the technological and policy landscape for the Internet of Things ("IoT").[1] TIA, representing the global community of information and communication technology ("ICT") manufacturers, vendors, and suppliers, believes the future of telecommunications and the world economy lies with IoT. It holds great potential for positive innovations across all market sectors within the United States and around the world. We believe it is important for the U.S. government to position its policy efforts in a way that allows consumers and businesses to fully capitalize on IoT's immense potential. A key foundation to the developing the proper policy approach is having a coordinated government understanding of the technologies, capabilities, and issues surrounding the IoT landscape. Thus, we commend the Commerce Department for inquiring into the role of the government in fostering IoT advancement.

TIA is a global trade association representing hundreds of manufacturers, vendors, and suppliers of ICT. On behalf of its members, TIA engages on policy matters that impact the opportunities, investments, and innovations that bring ICT services and solutions to businesses and consumers around the world. In addition, TIA serves as an accredited standards development organization ("SDO") for the telecommunications industry, housing efforts that address industry-consensus needs across the communications space, including machine-to-machine ("M2M") communications, telecommunications cabling systems, public safety and business/industrial radio communications, and others.

As an ANSI-accredited SDO, TIA engaged in the development of technical standards for the IoT landscape. TIA houses standardization efforts, such as its Engineering Committees TR-48 (Vehicular Telematics)[2]; and TR-50 M2M (Smart Device Communications).[3] TIA is also involved with oneM2M, an international partnership with European and Asian partners

[1] NTIA Request for Public Comment on The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, 81 Fed. Reg. 19,956 (Apr. 6, 2016).

[2] Engineering Committee TR-48 is responsible for the development and maintenance of voluntary standards relating to vehicular telematics equipment and services and intended to be employed in support of vehicular telematics.

[3] Engineering Committee TR-50 M2M (Smart Device Communications) is responsible for the development and maintenance of access-agnostic interface standards for the monitoring and bi-directional communication of events and information between M2M systems and smart devices, applications or networks. These standards development efforts pertain to but are not limited to the functional areas as noted: Reference Architecture, Informational Models and Standard Objects, Protocol Aspects, Software Aspects, Conformance and Testing, and Security.

working to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software.[4]

TIA members are developing an array of innovative technologies that cut across the IoT landscape and the different market segments to facilitate more efficient, data-driven consumer, enterprise, and government endeavors. The ICT industry is continuing to work towards realizing this continuum of connectivity that will serve as the core of IoT operations and we encourage NTIA, the Department of Commerce as a whole, and the broader U.S. Government to proceed cautiously as it considers its role in this space. Policies grounded in the fundamental principles of competitive- and technology-neutrality will be the most effective way to ensure that the IoT ecosystem is able to thrive and yield the full possible benefits.

II. TIA'S RESPONSE TO SPECIFIC TOPICS RAISED BY NTIA

A. General

Our society is in the midst of a dramatic transformation from the use of isolated systems to one centered on Internet-enabled devices that can network and communicate with each other and the cloud. This new norm where most everyday consumer and enterprise devices will be connected and able to collect data is the thrust of the Internet of Things. While TIA does not aim to define the concept of IoT, we believe that the core attributes as outlined in our 2015 White Paper on "Realizing the Potential of the Internet of Things"[5] are crucial to any established government definition of the term.

At its most basic, the Internet of Things is a label for the concept of an increasingly connected future in which regular, everyday items – from household appliances to cars to medical devices – are outfitted with sensors and connected to the Internet to share their data. Viewed more broadly, the Internet of Things will give rise to an entire ecosystem for interconnected devices, objects, systems, and data all working together. In this new world, most communications will be machine-to-machine ("M2M"), and there will be a continuous exchange of information between devices, sensors, computers, and networks.

In reviewing the two U.S. Government efforts to define IoT or similar concepts cited by NTIA, both seem to capture the essential elements of IoT, connectivity, physical devices, and

[4] http://www.onem2m.org/

[5] Telecommunications Industry Association, White Paper, *Realizing the Potential of the Internet of Things: Recommendations to Policy Makers*, (2015), *available at* http://www.tiaonline.org/sites/default/files/pages/TIA-White-Paper-Realizing_the_Potential_of_the_Internet_of_Things.pdf.

smart sensing.[6] The FTC definition[7], however, is more understandable for the regular user and consumer of these services and products; the NIST definition[8] does not seem to acknowledge the fact that the physical systems involved are non-traditional to the computing or connectivity environment. This definitional difference is likely inherent to the distinct intended audiences for the documents. Thus, it may be useful for the U.S. Government to consider the audience and intended purpose of any future effort to establish an accepted definition for policy purposes.

IoT is serving as a disruptive force because at the core it is about the ability to collect and analyze huge volumes of data. In the new IoT-driven world, there will be a continuous exchange of information between everyday devices, infrastructure, computers, networks, and people. It will raise some policy challenges similar to those presented by earlier computing transformations but the scale and volume of data as well as the continuous transactions envisioned in a future where IoT has met its full capability will be unlike any other time in history. For the efficiencies, ease of use, and many other benefits to be actualized, IoT systems must be able to handle the transmission, receipt, and processing of exponential amounts of data within countries and across borders in a seamless manner.

The penetration of increasingly connected devices (via Internet adoption and faster mobile connections) and the availability of advanced computing capability with significant processing power are enabling the growth of IoT. The increased availability of low-cost sensors will also help expand the potential market for IoT deployments and services, as cost issues are not expected to be significant. IoT systems will collect real-time data and transmit it via the Internet or wireless networks to computers, other machines, or to people. At the receiving end, application software is analyzing the data and converting it to useful information. This ability to collect and analyze huge volumes of data is the aspect of the Internet of Things that will be truly transformative. With virtually any device becoming IoT-capable and significantly increased analytics capability, government, consumers and businesses can make decisions that are more efficient and develop new business models which maximize the value of data.

[6] *See* FR Notice at 19,958, fn. 8. The Federal Trade Commission's report as well as the 2015 CPS Draft Framework defines "IoT" as primarily about connected networks of parts producing data.

[7] *See* Federal Trade Comm'n, *Internet of Things: Privacy and Security in a Connected World*, FTC (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[8] *See* NIST Cyber Physical Public Working Group, *Framework for Cyber-Physical Systems* (May 2016), https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Draft_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf.

Another differentiator for IoT is the major role that systems involving strictly M2M communications will play. It is important to understand that M2M equipment is often designed without any capability for physical human interaction or use. Something like an irrigation monitor is not intended to be accessed by humans because the focus is on data collection, analysis and possible automated response. Therefore, these types of devices will not have screens or keyboards or what the average consumer might experience with traditional computing devices. The distinction is important to understanding how certain enterprise IoT devices and systems function and the similarities and differences to more commonly understood IoT operations. This highlights how important it is for policymakers to understand the full landscape of services and capabilities that may exist in the IoT ecosystem to ensure policies are appropriately fitted to each situation.

IoT is clearly in its nascent stages, and holds great potential. IoT will utilize the gamut of network approaches and architectures, and given the wide range of services and solutions envisioned by the IoT, no particular network configuration can serve as the "best" solution. The IoT of the future will exist on an ever-advancing infrastructure and will need to utilize technology and devices that are both wireline and wireless as well as both legacy and cutting-edge. It will be important to focus on accelerating the development and deployment of all intelligent devices (existing and future) – essentially creating "systems of systems" – by horizontally connecting the edge of IoT solutions to the cloud, and enabling end-to-end analytics to transform services. A successful end-to-end strategy will make existing devices more intelligent and secure to reliably filter and manage data locally, so that they can seamlessly interact with each other as well as with new IoT devices and infrastructure in the future across industry sectors.

Furthermore, the new IoT model will include a variety of service and industry participants in the ecosystem, well beyond the traditional framework for telecommunications. Historically, the business model involving communications technologies has included device manufacturers, service providers, and the end user. In today's environment and as we move towards the fully-realized IoT future, there will be a multi-layered collection of companies working to deliver IoT solutions. These new players will include cellular providers, device and data management providers, analytics solution providers, system integrators, data storage/cloud service providers, and many more. Therefore, policymakers will need to be cognizant of how IoT operations work in various sectors and industries to ensure their rules consider and take into account the interests and implications of the much broader set of stakeholders.

We encourage NTIA to adopt a policy approach that incentivizes investments in the network, infrastructure, and promotes research to demonstrate the actual benefits of IoT services across the various market sectors. The policy approach should also focus on horizontal policy issues that arise in all the vertical markets, as discussed in the section II C below, before pursuing any vertical market-segmented policy.

B. Technology

As NTIA states, "[t]echnology is at the heart of IoT and its applications."[9] The varied and wide reach of IoT applications are such that it will need to be powered by a host of different technology capabilities targeted at specific functionalities. The technological needs for IoT services focused on "things" in the home or other locations that are stationary and involve short connection ranges will differ significantly from applications that involve regular location change and travel over a longer distance. To facilitate and promote the full spectrum of IoT offerings, it is imperative that policymakers employ an approach that adheres to principles of technology neutrality. The U.S. Government should avoid any situation that would place a government actor in a position to determine the future design and development of technology.

Policymakers should be wary of taking an action that would favor one technological approach over another as the various network and edge products and services will ultimately succeed or fail based on their ability to achieve projected values and meet consumer needs. Ultimately, the most appropriate role for the government as it relates to technology will be policies that consider the relevant needs, risks, and benefits of various stakeholder entities – consumers and industry; public and private; enterprise and government – to further a balanced outcome.

Network Technologies

A specific technological element that will be important to buttressing IoT development is the underlying network. We encourage NTIA and the U.S. Government as a whole to recognize the significant role that the network plays in the future envisioned by the seamlessly connected IoT future. While edge services and applications are important, an inordinate amount of the responsibility to enable these operations will rest with the network and devices that enable these functionalities. Thus, to achieve NTIA's stated goal of fostering IoT innovation and growth, governments across the globe will need to adopt policies that incentivize research and development ("R&D") for innovative solutions on how to increase network capabilities and maximize the use of limited resources like spectrum.

[9] FR Notice at 19,958.

Establishing an appropriate spectrum policy will be critical as its use is important to both consumer and government activities. Radio technologies are changing, placing new demands on spectrum allocations and raising new operational and regulatory challenges. Spectrum allocations and uses will need to be:

- **Predictable:** identifying demand and changes in demand while also understanding the pace of radio technology development by platform and making a long term plan;
- **Flexible:** policies consistent with baseline technical rules that are tech-neutral; allow for licensed and unlicensed uses;
- **Efficient:** encourage more efficient use of spectrum where technically and economically feasible; protect licensed use from harmful interference; place similar services in adjacent bands; and allocate wide, contiguous blocks of spectrum;
- **Prioritized:** where spectrum sharing is technically and economically feasible, policies should advance good engineering practice to create an environment that protects superior rights.

IoT will rely significantly on maximizing continuity of connectivity. Continuous connectivity will be required as users move geographical locations and over an extended period time for individual use sessions and over the lifetime of IoT hardware. However, there will be no one size fits all technology for IoT; rather, the varied technological mediums for connectivity will have a role and consideration of this factor is necessary for policymakers. IoT will need to utilize both wireline and wireless technology, and both legacy and cutting edge components of each. Currently, both wireline and wireless networks are transitioning to more IP-based technologies which offer numerous benefits to both enterprise and consumers. However, as 4G/LTE networks are increasingly being deployed there will likely still be a need, and a role, for 3G networks in IoT deployment. Consideration must also be given to the future 5G network, which is still being conceived and holds many yet untold possibilities. Similarly, Wi-Fi, satellite, Bluetooth, and a host of other communications technologies will be playing a role and seeking to compete in this marketplace.

TIA believes that many of the Federal Communications Commission's efforts surrounding spectrum policy are on the right track. It seeks to balance the interest in various spectrum uses while attempting to reorganize bands to achieve many of the principles outlined above. We are particularly encouraged by the *Spectrum Frontier* proceeding[10] which seeks to respond to the expanding demand for additional spectrum that can serve not only traditional mobile broadband applications but also many of the emerging needs that are

[10] Use of Spectrum Bands Above 24 GHz for Mobile Radio Services, GN Docket No. 14-177, IB Docket Nos. 15-256, 97-95, WT Docket No. 10-112, RM-11664, *Notice of Proposed Rulemaking* (2015).

happening because of the Internet of Things. Although spectrum above 24 GHz will not be the sole solution to the demand for spectrum-based services, the potential availability of large contiguous swaths of spectrum above 24 GHz makes the millimeter wave bands ideal for meeting many of those needs that can be addressed within the limits imposed by the bands' propagation characteristics and the state of technology.

In addition to the wireless networks, IoT solutions will rely heavily on wired media particularly for certain industrial applications. High-capacity, low-cost cabling solutions that allow the connection of a multitude of increasingly sophisticated individual sensors to the network will often be essential for quality-of-service or security reasons where wireless options do not make sense. Wired solutions also avoid the spectrum bandwidth constraints associated with widespread deployment of individual sensors or devices. Cabling could potentially be used for powering individual sensors or devices, making it essential for applications where the use of individual device batteries would be difficult.

Interoperability and Standards

Another major driver of IoT's success will be the interoperability of the global ecosystem. The development of open, voluntary, consensus-based global standards that will pave the way for devices to seamlessly connect to each other and to the network in an interoperable manner is critical. Thus, standards will be a key factor in the technological component of IoT success. However, the standards that are decided on should be directed by the participants in standards development organizations not a government body. Currently, there are a variety of ongoing and often competing standardization efforts. TIA generally supports this multiple path approach as the best process for spurring innovation and ultimately letting the public and market identify which most effectively meets society's needs. As discussed below, this is one area where horizontal policy consideration is necessary because we expect that standards in this space will be developed in a way that they can be applied across market sectors, for various end uses, and across countries.

Standardization is a form of economic self-regulation and therefore can relieve the government of the responsibility of developing detailed technical specifications while ensuring that voluntary, consensus standards serve the public interest. We encourage NTIA and its government counterparts to defer to these standards, which can be a valuable source of scientific and technical information developed with the assistance of private sector experts. The U.S. Government can also help encourage the development of industry standards by funding research, particularly in cross-cutting and heavily debated areas like cybersecurity.

C. Policy Issues

As briefly discussed above, government intervention in the IoT marketplace should be only in cases where a large number of stakeholders have demonstrated that there is an economic and/or public interest need for government involvement. U.S. policymakers should ensure that some key principles serve as the foundation of any policy efforts. First, the U.S. government should adhere to competition- and technology-neutrality principles. As ICT manufacturers and vendors work to meet the needs of their customers, competition will ultimately determine which products and services succeed or fail in the market, thereby fueling further innovation. We encourage NTIA and its regulatory counterparts not to rush forward with policy that will stifle innovation and investment.

There are new innovations and solutions being developed and conceived therefore, U.S. policy needs to integrate sufficient flexibility such that the IoT market is not locked into specific set of solutions. To do otherwise would create a dynamic that would negatively impact the interoperability and standards that are needed for IoT proliferation. We strongly encourage the U.S. Government to promote an environment where competition and innovation can thrive by adopting regulations, if determined to be necessary, that are outcome-based.

Horizontal Policy Framework

Furthermore, the Internet of Things is already having major disruptive effects across a number of market sectors even though much of the technology and potential effects are still in the nascent stages of development and deployment. Vertical markets that will be affected by IoT include health care, transportation, energy, manufacturing, and government. Currently, IoT technology development is happening in a way that is causing the lines between these different market segments to blur in many instances. Nonetheless, policy discussions related to technologies and applications squarely within the IoT ecosystem have been executed in a vertical fashion, with policymakers focusing on adopting market-specific policies. Often, the discussions on things like smart grid, intelligent transportation, self-driving cars, wearables, and many other connected devices seem to happen in separate silos without much recognition that they are part of the larger Internet of Things. As NTIA notes, no agency has taken "a holistic, ecosystem-wide view" with regard to IoT policy[11] and we are encouraged by the agency's recognition of the flaws with such an approach.

Policies developed with an eye towards one vertical will undoubtedly, even if unintended, have implications for practices and approaches to other aspects of the IoT

[11] FR Notice at 19,957.

ecosystem. Thus, TIA believes regulators and legislators should adopt a policy approach that begins with a common horizontal framework whenever possible, followed by tailoring for specific vertical applications where necessary. In TIA's IoT White Paper, we outline a number of important horizontal policy issues that affect IoT across markets and use cases, including:

- **Interoperability.** Enabling devices and systems to connect with each other on a technical level, typically through reliance on common standards or protocols.
- **Privacy.** The ability of consumers and businesses to safeguard their own personal or business data in a world of machine-to-machine transmissions.
- **Security.** Ensuring that devices, networks, and applications are secured from threats by malicious actors.
- **Data storage**. Where, how, and when the vast amounts of data generated from individual sensors and devices will be stored.
- **Spectrum and Bandwidth.** Ensuring that sensor-enabled and network-aware devices are able to transmit their data in a manner that uses constrained resources efficiently.

These common threads running across IoT applications and use cases demonstrate the significant concern presented by vertical regulations imposed in one market that may be inappropriate for another. Therefore, to avoid a balkanized regulatory approach and encourage innovation, policymakers should pursue the areas of policy that have horizontal implications in a coordinated manner. The U.S., through the Commerce Department, should develop a mechanism for regular discussion among regulators across agencies whose focus area will be impacted by the Internet of Things.

Security

Since IoT naturally means an ever-increasing number of "things" being connected throughout society, new and evolving security concerns are emerging across the various market segments with particular interest being paid to cybersecurity for connected health devices and cars. ICT companies are not blind to sensitivities surrounding consumer and government concerns about cybersecurity. In fact, security issues are often considered throughout the product development and design cycle, with many companies employing security by design principles. TIA members continue to take appropriate organization-specific steps to guard against and respond to the evolving threat landscape and they recognize the ability to advertise efforts to secure their products and services as key to success in the IoT marketplace. This approach will continue to mitigate threats as the IoT develops and proliferates. TIA urges policymakers to regard IoT as an opportunity for greater security, since using a network approach paired with proper risk management techniques will enable

IoT devices to work together to produce comprehensive, actionable security intelligence in near real-time.

The ICT industry believes that encryption will need to be a key component of the discussion about promoting security in IoT. We believe it is imperative that lawmakers recognize that attempts to promote and further IoT advancement will inherently require industry to adopt and use forms of encryption in certain services and communications in order to help bolster consumer trust. Encryption is one of the most important tools that companies have at their disposal to help combat security challenges and be responsive to concerns being raised both by the consumers and government officials about our connected future. TIA believes there will be a need and role for the use of varying levels of encryption throughout the IoT ecosystem.

We recognize the sensitivities of the ongoing policy discussion about how to effectively balance virtual privacy and security interests with similar physical interests. As with every new and emerging technology, this issue will require continued conversations between technical and policy experts and we are encouraged by some of the government efforts trying to enable that. TIA asks that government officials not adopt a policy posture that would result in outright restrictions on the use of secure, encrypted protocols or force companies to weaken their security measures. That kind of policy approach would be harmful to the ultimate success of IoT. TIA emphasizes the need for nuanced assessments of the multiple factors at play.

With respect to matters of security, TIA recommends that policymakers not develop heavy-handed regulations that are not able to keep pace with the constantly evolving threat and risk landscape. Rather, the preferred role for government is to work with industry to help identify risks and respond to threats through the use of public-private partnerships ("PPP"). The PPP model has proven to be an effective tool for collaboration on addressing current and emerging threats, and will serve as a key incentive for encouraging businesses to invest in security in a way that is most appropriate for their business and the risks they face. TIA applauds the Commerce Department for its use of and recognition of the value of the PPP approach which has been employed many of its sub-agencies (e.g. NTIA, NIST) to address a host of issues.[12] It is apparent that the Commerce Department recognizes the importance of having various stakeholders at the table and finding a way to lead policy in a coordinated

[12] Over the years, there have been a number of policy initiatives undertaken by Commerce Department entities that have as their foundation the idea that public private partnerships or broader multistakeholder discussions are the key to solving important policy matters. Some examples of this include NIST's efforts to develop the Cybersecurity Framework, the recent Cyberphysical systems framework as well as the variety of NTIA multistakeholder processes on issues like privacy, facial recognition technology and cybersecurity vulnerabilities.

fashion rather than employing a heavy-handed top-down approach. Where industry collaboration is not moving forward at an appropriate rate to address significant national needs, the Government can use its convening power to bring stakeholders together, as NTIA and other Commerce sub-agencies have done.

As discussed in the section on technology, standards activity is also crucial to addressing the issue of security. Numerous standards, guidelines, best practices, and tools are used by the ICT industry to understand, measure, and manage risk at the management, operational, and technical levels. Policymakers should ensure that their approach to IoT reflects the priority of the development of internationally-used standards and best practices. The global nature of the industry necessitates the role of a global approach to cybersecurity concerns rather than adopting country-specific standards. There are legitimate concerns regarding the issue of security as all aspects of our society become more connected but any regulations on this issue should focus on performance requirements rather than choosing a specific standard or technical specification.

Supply Chain

An area of policy that needs more attention in IoT policy discussions is the facilitation of the role of the global supply chain of products and services in this space. ICT is playing a significant role in enabling the IoT future. ICT has a supply chain that is globally diverse with parts being manufactured, supplied, and put together from various areas across the globe. TIA members are technology leaders that develop and integrate hardware, software solutions, and ICT products, that will play a critical role in improving the efficiency and usability of many services and products enabled by IoT. Thus, U.S. policy should take care not to restrict the ability of global companies like ICT manufacturers and suppliers to compete for and have their products be acquired to support the IoT ecosystem through access to federal grants and R&D funds. U.S. policy should ensure that recipients of federal funds are not limited in the types of technology they can procure due to extremely rigid Buy America provisions.

Currently, there is a U.S. policy that ICT has traditionally been exempted from Buy America requirements. For example, in 2009, NTIA issued a formal exception for these technologies as it related to the Broadband Technology Opportunities Program (BTOP).[13] As NTIA noted at the time, the manufacturing supply chain for ICT products that support broadband infrastructure is varied and consists of components that are developed around the world. We ask that as the government considers ways to promote IoT it ensures that similar exemptions are in place and applicable to grant programs across the various market segments

[13] *See* NTIA Buy American Exception under the American Recovery and Reinvestment Act, 74 Fed. Reg. 125 (July 1, 2009).

that would be benefited by the role of IoT solutions. This kind of waiver is critical as the government considers new grant and funding opportunities to advance IoT development in the U.S. , whether for Smart Cities generally or targeted to specific market sectors. These targeted waivers will help facilitate use and development of the most advanced technology solutions in communities across the country and ultimately be in the best interest of the American public.

D. International Engagement

The U.S. Government should employ regulatory approaches that are globally harmonized, transparent and streamlined. The marketplace for ICT goods is not cordoned off by geographic or country borders; therefore, polices and regulations for ICT should be harmonized, predictable, transparent, and reliable to promote the "build once, sell anywhere" model. This model will ensure the continued growth of the IoT marketplace by reducing regulatory costs, time-to-market, and costs to end users through the business and consumer markets.

There are a number of foreign entities that have already begun to pursue and seek public input on the role of government in the Internet of Things. It would be useful for the U.S. Government to engage with those entities and identify opportunities for alignment. This effort will enable the Internet of Things to flourish by removing geographic barriers when possible to how governments consider, regulate, and promote the IoT ecosystem. Many of the technological and policy issues discussed above will have to be addressed across the globe and policy activity that facilitates cross-border coordination will be crucial to furthering IoT advancement.

III. CONCLUSION

The IoT technological revolution presents boundless potential benefits for our society. TIA believes it is important for the U.S. Government to have a coordinated government understanding of the technologies and service offerings that are encapsulated in IoT to inform any policy considerations. We support the Commerce Department's effort to follow a path that is thoughtful, collaborative, and pro-innovation, consistent with the specific recommendations above, and we look forward to future engagement on these important items.

Respectfully submitted,
By: /s/ James Reid
Avonne Bell
Telecommunications Industry Association
abell@tiaonline.org