Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
U.S. Department of Commerce
Washington, DC 20004

In the Matter of:	)	
	)	
The Benefits, Challenges, and Potential Roles	)	Docket No. 170105023-7023-01
for the Government in Fostering the Advancement	)	
of the Internet of Things	)	RIN 0660-XC033

COMMENTS OF THE
TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Telecommunications Industry Association ("TIA")[1] welcomes the opportunity to comment on the National Telecommunications and Information Administration ("NTIA") green paper entitled "Fostering the Advancement of the Internet of Things."[2] Having a coordinated government understanding of the technologies, capabilities, and issues surrounding the IoT landscape is essential to developing policy approaches that will allow consumers and business to fully capitalize on its immense potential. We therefore commend NTIA for its continuing inquiry into the role of the government in fostering IoT advancement.

I. The Role of TIA and Our Members in the Internet of Things

In addition to policy advocacy, TIA serves as an accredited standards development organization ("SDO") for the telecommunications industry. TIA houses 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 has developed technical standards for the IoT landscape. TIA houses standardization efforts within its Engineering Committees such as TR-48 (Vehicular Telematics)[3] and TR-50 M2M (Smart

[1] TIA is the leading trade association for the information and communications technology ("ICT") industry, representing companies that manufacture or supply the products and services used in global communications across all technology platforms. TIA represents its members on the full range of policy issues affecting the ICT industry and forges consensus on industry standards.

[2] NTIA Notice and Request for Public Comment, *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, 82 Fed. Reg. 4,313 (Jan. 13, 2017)

[3] 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.

Device Communications).[4] TIA is also involved with oneM2M, an international partnership with European and Asian partners 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.[5]

TIA members are developing an array of innovative technologies that cut across the IoT landscape and 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. Thus, 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 fundamental principles of competitive- and technology-neutrality will be the most effective way to ensure that the IoT ecosystem thrives and yields the fullest possible benefits.

II. Broad Engagement

As TIA outlined in our 2015 White Paper on "Realizing the Potential of the Internet of Things,"[6] our society is in the midst of a dramatic transformation from the use of isolated systems towards Internet-enabled devices that can network and communicate with each other and the cloud. This new normal in which most everyday consumer and enterprise devices will be connected and able to collect data is the thrust of the Internet of Things.

For that reason, we applaud NTIA efforts to engage IoT stakeholders in the broadest sense. This outreach appropriately includes 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.

For these reasons, we also believe regulators and legislators should adopt a policy approach that begins with a common horizontal framework whenever possible, followed by

---

[4] 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.

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

[6] 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.

tailoring for specific vertical applications where necessary. A coordinated whole-of-government approach that includes the numerous government agencies with a stake in the advance of IoT should be a priority – whether from a transportation, communications, energy or cybersecurity perspective.

III. Technology Neutrality

"Continue to foster an enabling environment for IoT technology to grow and thrive, allow the private sector to lead, and promote technology-neutral standards and consensus-based multistakeholder approaches to policy making at local, tribal, state, federal, and international levels on issues ranging from U.S. security and competitiveness."[7]

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 decide the future design and development of commercial 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 commercial technology will be policies that consider the relevant needs, risks, and benefits of various stakeholder entities – consumers and industry; public and private sectors; enterprise and government users – to further a balanced outcome.

IV. Continuity of Connectivity

"Meeting these connectivity demands will require continued modernization of legacy telecommunications infrastructure and buildout of additional broadband capable networks. A percentage of the current telecommunications networks were primarily built for voice service and historically were largely copper-based." [8]

IoT will rely significantly on maximizing continuity of connectivity. Continuous connectivity will be required as users move between geographical locations and over an extended period of 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 that offer numerous benefits to both enterprise and

[7] NTIA Green Paper at 42.

[8] *Id.* at 16.

consumers. In the case of terrestrial wireless networks, while 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 as-yet-untold possibilities. Similarly, Wi-Fi, satellite, Bluetooth, and a host of other wireless communications technologies will be playing a role and seeking to compete in this marketplace.

One 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.

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 are not viable. Wired solutions also avoid spectrum 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.

V. Spectrum Policy

"Continue to innovate in spectrum management to increase access to spectrum that will help facilitate IoT growth and advancement. NTIA, through its Office of Spectrum Management, will collaborate with stakeholders, including its spectrum-related interagency (Policy and Plans Steering Group and Interdepartmental Radio Advisory Committee) and external advisory bodies (Commerce Spectrum Management Advisory Committee), to assess the spectrum implications of the diverse IoT applications that currently or in the future may be delivered through a number of technologies operating in various spectrum bands."[9]

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. In general, spectrum allocations for all technologies and associated investments 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;

[9] *Id.* at 23.

- **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.

We believe that many of NTIA's efforts surrounding spectrum policy are on the right track. The agency has sought to balance the interest in various spectrum uses while attempting to reorganize bands to achieve many of the principles outlined above. For example, the agency has leveraged the expertise of the Commerce Spectrum Management Advisory Committee ("CSMAC"), has published a compendium of federal government spectrum bands, and has recently released quantitative assessments of usage in five targeted spectrum bands spanning 960 MHz.

Meanwhile, at the FCC we are particularly encouraged by the *Spectrum Frontiers* 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 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 the needs that can be addressed within the limits imposed by the bands' propagation characteristics and the state of technology. Work is currently being done to determine how this spectrum can be shared with existing and planned technology investments.

VI. Interoperability and Standards

Industry, with active participation from government experts as needed, is ideally positioned to lead the development of technological standards and solutions to address global IoT environment opportunities and challenges.[11] *….The Department of Commerce agrees with commenters that an industry-led, bottom-up, consensus-based approach to standards development is necessary to realize the benefits of the technology.*[12]

Another major driver of IoT's success will be the interoperability of the global technology 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.

---

[10] Federal Communications Commission, *Use of Spectrum Bands Above 24 GHz for Mobile Radio Services*, GN Docket No. 14-177.

[11] NTIA Green Paper at 45.

[12] *Id.* at 47.

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. 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.

However, standards development should be directed by the participants in standards development organizations, not by government bodies. 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. 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.

VII. Security

"This emphasis on a risk-based approach conforms with a broader focus across the Department on understanding and addressing cybersecurity risks in the business/mission context.[13] ** * * The Department will continue to bring private sector experts together with policymakers to define security principles for IoT, facilitate IoT security framework development by sector and application, and encourage the implementation of best practices and/or minimum standard.*[14]

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 very familiar with both consumer and government sensitivities about cybersecurity. In fact, security issues are often considered throughout the product development and design cycle.

TIA members continue to take appropriate organization-specific steps to guard against and respond to the evolving threat landscape. Moreover, 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.

Information sharing. Fighting any fraud, malware or misuse of data within the IoT ecosystem will be necessary. To that end, we urge the federal government to facilitate a

[13] *Id.* at 26.

[14] *Id.* at 40.

dialogue/discussion about information sharing of fraud indicators and response and recovery methodologies. With the increasing sophistication and scale of the fraudster operations, the rapid sharing of threat indicators across all vulnerable networks is critical.

Encryption. 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.

Flexible approaches. 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 such conversations. 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. Instead, we emphasize the need for nuanced assessments of the multiple factors at play.

We also recommend that policymakers not develop heavy-handed regulations that are not able to keep pace with the constantly evolving threat and risk landscape. For example, rapid legislative responses to high-profile breach events in the IoT space might ultimately undermine security rather than promote it. 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 by various sub-agencies (including NTIA and NIST) to address a host of issues.[15] 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 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,

[15] 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 multi-stakeholder discussions are the key to solving important policy matters. Some examples of this include NIST's efforts to develop the Cybersecurity Framework, the recent Cyber-physical systems framework as well as the variety of NTIA multi-stakeholder processes on issues like privacy, facial recognition technology and cybersecurity vulnerabilities.

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.

Finally, 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.

VIII. International Engagement

"Government-to-government dialogues and relevant international fora are major vehicles for the Department's international engagement on IoT. Currently the Department maintains formal dialogues with numerous governments where digital economy and general information and communications technology issues are often discussed."[16]

The U.S. government should seek to export its policy and regulatory approaches in this space in a way that drives a more globally harmonized, transparent and streamlined result, benefitting U.S. interests overall. 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.

A number of foreign governments have already begun to pursue and seek public input on the role of government in the Internet of Things.[17] TIA would encourage the U.S. Government to engage with them to 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.

---

[16] NTIA Green Paper at 40.

[17] *See, e.g.,* OFCOM (United Kingdom), *Promoting Investment and Innovation in the Internet of Things* (2014-15), *available at* https://www.ofcom.org.uk/consultations-and-statements/category-1/iot; European Commission, *Advancing the Internet of Things in Europe* (Apr. 4, 2016), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0110&from=EN.

IX. 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 federal 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,

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

By: /s/ *Dileep Srihari*

Cinnamon Rogers
Dileep Srihari
Telecommunications Industry Association
1320 N Courthouse Rd Suite 200
Arlington, VA 22201

March 13, 2017