TRANS-ATLANTIC BUSINESS COUNCIL

June 3, 2016

RE: Request for Comment from the National Telecommunication and Information Administration (NTIA) on "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things"

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?*
   a. *What are the novel technological challenges presented by IoT relative to existing technological infrastructure and devices, if any? What makes them novel?*
   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?*
   c. *What are the most significant new opportunities and/or benefits created by IoT, be they technological, policy, or economic?*

With the new advancements surrounding the Internet of Things (IoT), as with many fast moving technologies, challenges exist for policy makers. The U.S. needs a common, integrated cross-sectorial approach across technologies to support industry's further digitalization. Efforts need to be made to build integrated industrial systems rather than initiatives that could create fragmented silos when addressing new technological and regulatory fields like RFID, IoT, Cloud Computing, and "Advanced Manufacturing". All of these technologies and related initiatives are components of the future digital environment and require cross-sectorial coordination across policy makers and industries.

To ensure advances in IoT deliver on expected benefits, governments should promote an enabling public policy environment that does not prevent innovative solutions before their merits can be tested in the marketplace. Novel challenges will arise in several key areas: continued investment in high-speed communication; sufficiently harmonized spectrum resource should be made available; robust and context-appropriate data protection regulation that guarantees the privacy of the citizen without hampering innovation; support for the market-based and industry-driven standardization model enabling standards to be developed in the standards developing organizations (SDOs) most relevant to the specific issues being dealt with in each standard; and creation of appropriate education, and training and certification programs to ensure that labor force's skillsets are kept up to date and to educate regulators to appropriately address IoT developments.

IoT will allow for new data-driven insights allowing industry to deliver new, innovative services and products. With this will bring new information like big data coming from a multitude of devices and systems that will require new entities to collect, secure, analyze and integrate this data. This IoT must also be scalable and on a secure platform that can be managed according to standards. All devices will also need to be able to work together and integrate with other devices, communicating seamlessly with all connected systems and infrastructure.

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?*

There is no universal definition as IoT represents an evolution of technology, process and policy which has occurred over the last 25 years. In the late 1990s, researchers at Xerox Parc lab were working on concepts of ubiquitous computing, which came to represent a model of a highly interconnected and networked future: interconnection of people, objects and services in computer aware environments. In the early 2000s, Asian policy makers were using the phrase liberally in the Asia-Pacific Economic Cooperation (APEC) and demonstrations of the "house of the future" were being built globally. Over time, technology and applications have developed to make this more of a reality. Machine to Machine (M2M) solutions have pushed the limits of non-human mediated communications to new capabilities, and the infrastructure of the Internet of Things (IoT) has progressed with significantly more ability to interact.

The primary concern of IoT is how to connect objects together at the network layer. This means creating network connectivity between products, goods, cars, sensors and other everyday objects. The term 'Internet of Things' (IoT) refers to the connection of devices and objects. In most cases, IoT services have a closed user group, whereby open internet or any-to-any voice communications are not the primary purpose of the service. This connectivity allows such products to generate and exchange data.

Any definition should be flexible enough to adapt as IoT further develops. In this sense, in its latest report1, BEREC (the body of European regulators) does consider the issue of definitions and concludes: *'For the purposes of this report, it is not necessary to determine in detail which definition is most appropriate. Fixing a definition of M2M communications or IoT services only makes a crucial difference if obligations explicitly depend on that distinction*".

3. *With respect to current or planned laws, regulations, and/or policies that apply to IoT:*

[1] BEREC (2016) - Enabling the internet of things available here

a. *Are there examples that, in your view, foster IoT development and deployment, while also providing an appropriate level of protection to workers, consumers, patients, and/or other users of IoT technologies?*
b. *Are there examples that, in your view, unnecessarily inhibit IoT development and deployment?*

Some key areas are worth noting:

- Security and privacy "by design" are key to ensure a confident and resilient IoT/M2M ecosystem as these services are very sensitive
- The viability of permanent roaming for M2M supports the growth of IoT.
- Taxing may deter the development of IOT. In Brazil, a tax reduction increased the take up of innovative M2M services. According to GSMA intelligence calculations as of December 2014 the M2M devices benefiting from the tax reduction have grown 26% against only 7% of other M2M standard devices.[2]

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.*

5. *Please provide information on any current (or concluded) initiatives or research of significance that have examined or made important strides in understanding the IoT policy landscape. Why do you find this work to be significant?*

In the U.S., Industrial Internet research and work is being led by the Smart Manufacturing Leadership Coalition as well as other numerous initiatives supported by the federal government[3]. U.S. industry is also looking to meet the new challenges of the digitalisation of industries. For example, in the spring of 2014, U.S. companies founded the Industrial Internet Consortium (IIC) to bring together all the relevant players across technologies to develop best-case practices, use cases, influence standards etc. IIC counts more than 120 members.

Technology:

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

[2] M2M in Latin America. State of the market available here: https://www.gsmaintelligence.com/research/?file=61597e051824446354a245fd5ed8a292&download

[3] Kurfuss, Thomas (December 2014). Industry 4.0: Manufacturing in the United States. *Bridges, vol 42*. http://ostaustria.org/bridges-magazine/item/8310-industry-4-0

a. *Examples of possible technical issues could include:*
    i. *Interoperability*
    ii. *Insufficient/contradictory/proprietary standards/platforms*
    iii. *Spectrum availability and potential congestion/interference*
    iv. *Availability of network infrastructure*
    v. *Other*

Allocation of sufficient spectrum in an internationally harmonized manner will be critical. Internationally harmonized spectrum is essential to enable wireless Machine-to-Machine (M2M)/IoT technology for global deployment, ensuring interoperability and driving down costs to increase economies of scale. Nevertheless, a balance should be reached between unlicensed and licensed spectrum avoiding any market distortions between both. This will enable spectrum sharing between M2M/IoT applications, driving spectrum efficiencies, helping promote innovation and competition. Some M2M/IoT services usually have very long life cycles based on 2G/3G technologies. There will be an increasing need for international spectrum coordination to adequately protect these services from any disruptions worldwide.

With the expected explosion of M2M/IoT devices, sufficient identifying resources must be available (such as IP addresses and resource identifiers) to ensure there is structural capacity to accommodate newly connected devices. Flexibility is essential for numbering resources, including extra territorial and international global numbers as different services or users may have different requirements.

Today, local telephone numbers (E.164) are the most widely deployed numbering resource used to connect to mobile networks. Some traditional consumer protection requirements commonly associated with E.164 numbers are not needed or appropriate in the IoT context, for instance number portability, possibility to call emergency services and Calling Line Identification (CLI) rules. However, there is concern that M2M/IoT technology will subsume their availability.

International mobile subscriber identity (IMSI) numbers (E.212) offer a solution to increasing numbering resources. Government regulators should ensure that IMSI's or other suitable resource identifiers are permissible and interoperable with local mobile networks to enable traditional mobile and M2M/IoT growth. Note that international IMSIs issued in one country could be used "extraterritorially" via permanent roaming in a third country. In the context of M2M-services, it could prove very complex and costly to require operators to comply with registrations or approvals for use in third countries.

Policies providing an IPv6-friendly environment will also open an effectively limitless range of "things" to be globally addressed thus further enabling new IoT and M2M applications.Even if IPv6 will become the standard communications protocol, before we reach that stage resources such as IMSIs and (15 digit) MSISDNs continue to be necessary to offer connectivity to IoT.

The choice of the connectivity model depends on the expected footprint of the devices, e.g. connectivity could be achieved through an mobile network operator (MNO) who has roaming agreements in place or on a multi-national basis through the so-called embedded SIM Model, which enables the connectivity provider to be selected in the device distribution cycle. There is no "one size fits all" solution. For instance, a smart metering local application will have different requirements than a global parcel tracking system.

M2M/IoT tax burdens should be minimized as these services are usually characterized by very low Average Revenues Per User (ARPUs) and could harm seriously their current low profitability. Additionally, if any taxation or fee is required, it should be balanced across the M2M/IoT value chain.

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

Common approaches across technologies to support industry's further digitalization are vital to the development of IoT. Vision and an integrated cross-sectorial approach is necessary to ensure industrial leadership based on a fully digitized industry. Industry and policy should avoid fragmented silos when addressing new technological and regulatory fields

Government will be relevant not only as policy-maker and regulator but also as enabler and adopter. From ensuring compatible regulatory regimes on security and privacy to transparent and predictable market access regimes, public sector services must be leading adopters of emerging technologies.

Failure to recognize the interconnected and interdependent nature of these technologies and related business models may result in policy and regulatory frameworks that needlessly impede innovation through unnecessary burdens or unintended consequences. At a minimum, close coordination, collaboration and cooperation is required across all government policy makers and actors (both users and providers). This coordination, cooperation and collaboration needs to also extend across stakeholders to include businesses which develop the technology, its applications and related business models, as well as those that need to implement or use these technologies, including businesses and consumers/citizens/individuals.

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?

As the interconnection and interactivity has increased so has complexity. Where a main focus of interest in the early days of ubiquitous computing was radio-frequency identification (RFID) sensors, today the breadth of objects that can be connected and the information which can be provided or captured in real time has exploded. This variety and variability of information has also resulted in the emergence of concepts related to Big Data. Big Data represents not only a significant advance in the ability to capture and process data but also a significant progress in the ability to find correlations across these new and varied data sources as well as more sophisticated analytics to apply to them. Finally, Cloud Computing has evolved to provide numerous services which can be delivered with improved efficiency, economy, scope and scale, and which are completed by the increasingly rich and granular data and the related correlations and analytics.

Infrastructure:

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

Industrial Internet / M2M / Industry 4.0 require constantly available as well as high-performance communication infrastructures, with reliable and stable speeds providing advanced Quality of Service, short latency and short provisioning times. This can only be realized if quality differentiation in traffic delivery services is allowed. IoT will be dependent upon a robust cloud infrastructure able to manage new sensors, devices and data.

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?*

One example is that in the United States, net neutrality regulations do not apply to services that offer connectivity bundled with e-readers, heart monitors, or energy consumption. Another example of services excluded from the net neutrality regulations are limited-purpose devices such as automobile telematics. Therefore, the U.S. should ensure a well-balanced net neutrality regime that can secure the technical requisites associated to such innovative services needed in the current digitization of traditional industries.

One element that will be critical for the development of the Industrial Internet will be related to the ability for the commercial provision of seamless cross border services and the facilitation of the movement of data. For instance, compatible legal frameworks will allow efficiency of interconnected, cross border value chains.

10. *What role might the government play in bolstering and protecting the availability and resiliency of these infrastructures to support IoT?*

Strong incentives for continued investment in the U.S. in secure and high-speed communication infrastructure is necessary to meet the demands of a digital economy and the exponential

demands coming up in the Industrial Internet context in particular. There are significant differences in deployment and access to such infrastructure in different regions on both continents, with some areas well served and some not. These gaps must be closed to drive global competitiveness. By investing in new network infrastructures a strong ICT sector will follow, boosting efficiency, innovation, growth and employment across all sectors of the economy, But such investment must take place within a competitive telecommunications marketplace. This will help ensure that companies seeking to implement IoT technologies can do so in a way that protects their customers' data and delivers value along the entire internet value chain.

A common vision for the sector that would promote an equally flexible and investment-friendly regulatory environment is crucial. More emphasis is needed on policies that promote dynamic outcomes such as investment and innovation by all parties. Current regulatory frameworks were not created thinking of M2M/IoT services. Therefore policy makers should have a flexible approach to smoothly adapt current rules to innovative M2M/IoT services.

Governments and regulators should ensure a policy framework based on a light-touch, pro-competitive regulatory approach that incentivizes investment and enables the development of new business models for all players. Governments and industry members also need to continue to work to strengthen the protection of customer data. Regulation should also avoid technology restrictions given convergence trends (including telecoms-media) while relying on sustainable competition. Excessive or technology biased regulation can stifle innovation, raise costs, limit investment and harm consumer welfare

Economy:

11. *Should the government quantify and measure the IoT sector? If so, how?*
    a. *As devices manufactured or sold (in value or volume)?*
    b. *As industrial/manufacturing components?*
    c. *As part of the digital economy?*
        i. *In providing services*
        ii. *In the commerce of digital goods*
    d. *d. In enabling more advanced manufacturing and supply chains?*
    e. *What other metrics would be useful, if any? What new data collection tools might be necessary, if any?*
    f. *How might IoT fit within the existing industry classification systems? What new sector codes are necessary, if any?*

12. *Should the government measure the economic impact of IoT? If so, how?*
    a. *Are there novel analytical tools that should be applied?*
    b. *Does IoT create unique challenges for impact measurement?*

13. *What impact will the proliferation of IoT have on industrial practices, for example, advanced manufacturing, supply chains, or agriculture?*
    a. *What will be the benefits, if any?*
    b. *What will be the challenges, if any?*
    c. *What role or actions should the Department of Commerce and, more generally, the federal government take in response to these challenges, if any?*

14. *What impact (positive or negative) might the growth of IoT have on the U.S. workforce? What are the potential benefits of IoT for employees and/or employers? What role or actions should the government take in response to workforce challenges raised by IoT, if any?*

Policy:

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 the consumer/individual space ever more sensors are embedded or attached to devices including in things we wear, medical devices that may be implanted or the "smart" environments we may live and work in – appliances, cars, homes, grids and cities. In the business-to-business (B2B) space, the explosion of sensors and data has led to the Industrial Internet, which refers to the integration of big data analytics, IoT Machine-to-Machine services and cloud computing to enhance operational efficiency. This includes the interconnection of business objects that support healthcare delivery, service operations, supply chains, logistics, city planning, sustainable development and consumption - to name a few of the most important applications. Applying intelligence, applications and sectoral overlays build upon these uses to create the web of things, intelligent systems and Industry 4.0. We need common approach across technologies to support industry's further digitalization.

The concept of IoT consists of a number of known and applied standards and technologies - it should be supported by reliable and coherent policy, and (only) where necessary supported by a regulatory approach. As policy makers tackle these evolving technological trends in the policy sphere, considerations should be made to the following:

- To ensure advances like the Industry 4.0/Industrial Internet- powered by Machine to Machine (M2M) and IoT/WoT/WoS and Communications technology - deliver on expected benefits, governments should promote an enabling public policy environment that does not prevent innovative solutions before their merits can be tested in the marketplace.
- The U.S. rules on Open Internet/Net Neutrality should be implemented in a manner where operators are allowed to secure differentiated quality of services on their networks and to

conduct traffic management requirements accordingly, with the objective to support a variety of applications and services for Industrial Internet.

- Continued investment in the U.S. in secure and high-speed performance communication infrastructure is necessary to meet the demands of a digital economy. Governments and regulators should ensure a policy framework based on a light-touch regulatory approach that incentivizes investment in high-speed and ultra-fast communication networks and enables the development of new business models. Governments should ensure that the telecommunications marketplace is competitive. They should also ensure that sufficient harmonized spectrum resources are made available.
- Laws, policy frameworks and practices should provide for robust and context-appropriate data protection that guarantees the privacy of the citizen without hampering innovation. For example, companies should be aware that when they are collecting personal data from data subjects in the EU, it shall be handled in full compliance of the data protection law of the data subject. Both privacy and security concerns need to be appropriately taken into account in order to provide the needed trust environment with the involvement of all players.
- Sufficient identifying resources must be available (such as IP addresses and resource identifiers) to ensure structural capacity to accommodate newly connected devices.
- M2M/IoT tax burdens should be minimized.
- Maintain support for the market-based and industry-driven standardization model enabling standards to be developed in the standards developing organizations (SDOs) most relevant to the specific issues being dealt with in each standard.
- Policymakers should work with industry to assist in the creation of appropriate education, training and certification programs to ensure that labor force's skillsets are kept up to date and to educate regulators to appropriately address Industry 4.0/Industrial Internet's developments, products and services and other related emerging technologies.
- A level playing field policy should be applied in a technological neutral way. It is worth noting that the IoT value chain is extraordinary broader and more complex than only "cellular" or the mobile industry, including other kind of wireless access and diverse agents.

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

Security is critical across all uses of IoT technologies. While many of the security considerations are not new, there are unique challenges as these devices differ from tradition computing devices. The protection of proprietary information – like a manufacturer's supply-chain dashboard – is essential to ensure only authorized employees have access and prevent unauthorized individuals (inside or outside of the company) from copying or changing data. Policymakers, system owners, and system managers must consider the dynamic structure of systems that are distributed across multiple locations spanning the globe while transferring information between devices identified at times only by private IP addresses. In contrast to service providers managing information transfers between public IP addresses, managers of private IP networks must choreograph information flows within these systems using various data pipes from multiple suppliers across the entire geography of the private network. Security across applications is not absolute, but IoT security will range across a spectrum for devices.

Due to the intensive data exchange Industrial Internet/Industry 4.0 requires, it must be established on communication infrastructures that are robust and resilient in the face of cyber security threats. Therefore, most Industry 4.0 services and applications will run on corporate intra-nets, i.e. over dedicated intelligent networks, which ensure a secure environment (not the public internet).

The benefits of and reliance on IoT enhanced supply chains will only persist if the security needs of this new infrastructure are met. Global standards, good business practices and government policy and regulatory environments, particularly those that support competition, investment and innovation, all play a role in assuring this infrastructure. From a policy perspective, there is no need for a specific security approach, but the general aim should be to foster partnership through information sharing, incident response, awareness raising and global best practices.

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?*

A policy issue of great concern to individuals is the need to appropriately protect their personal data and provide assurances of privacy. Existing policy and regulatory approaches on data protection are already applicable to IoT, although concepts of how to apply those rules should be considered in light of the need to expand use of these technologies throughout economic sectors. As in all regulatory constructs, they should be applied in a consistent manner to enhance legal certainty. Furthermore, general data protection regulations should apply consistently across all IoT providers - mobile operators, device manufacturers, online platforms- in a service and technology-neutral way.

For instance, in Europe the General Data Protection Regulation aims to create a consistent horizontal level playing field for privacy standards among all players in the IoT, irrespective of technologies, infrastructure, business models and data flows involved or who provides a service or where a company or user is located.

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

This issue is predicated on the nature of the information being collected and used. We note that in many B2B/Industrial applications no personal data is involved and those applications do not raise privacy implications.

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?*

As regulators review the application of existing rules and data protection frameworks, they should examine them through the filter of the potential impact on the IoT. The IoT is characterized by data originating and combined from a variety of sensor based sources, from ubiquitous devices – a growing number without user interfaces – and free flow of data across devices and systems for individual and/or organizational applications. As such, data protection regulations should consider the context of data use and reasonable expectations of users, and not take overly-prescriptive approaches to purpose limitation, notice, consent, profiling and cross border transfer. Policy makers need to consider the context and develop frameworks that can enable those flows which pose no risk to privacy while assuring appropriate mitigation of risk on those that may implicate privacy or other individual interests. Industry should continue to work within cross sectorial associations as well as in partnership with policy makers to consider what changes may be required to practices of security and privacy in relation to evolving uses of these technologies.

18. *Are there other consumer protection issues that are raised specifically by IoT? If so, what are they and how should the government respond to the concerns?*

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?*
    b. *In what ways might IoT create obstacles for these communities or groups?*
    c. *What effects, if any, will Internet access have on IoT, and what effects, if any, will IoT have on Internet access?*
    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?*

IoT creates a new demand for convergence based skills combining classical engineering with electronics and software. This means new interdisciplinary teams and new individual skill profiles are needed which impact both education for new entrants to the workforce as well as up-skilling the existing workforce. A need for recognized certification programs also emerges. Furthermore, there will be a corresponding need to address skills of regulators to understand and address the needs of IoT products and services as they merge existing product categories.

Entrepreneurs will have to prepare their employees with high responsibility for the revolutionary changes the digitalization of production processes and enterprises will bring to the workforce. Policymakers should work with industry to accompany this development in assisting the industry at the creation of appropriate education and training programs to ensure the labor force's skillsets are kept up to date, in the context of IoT in particular also looking at the digital skills needs of non-ICT specialists.

International Engagement:

20. What factors should the Department consider in its international engagement in:
   a. Standards and specification organizations?
   b. Bilateral and multilateral engagement?
   c. Industry alliances?
   d. Other?

Modern standards are at the heart of this new industrial revolution. Market-based, industry-driven standards that are globally consistent permit the creation of interconnected, cross border value chains and allow them to function efficiently and without disruption. Such common standards should be agreed among as many partners in the U.S. and globally as possible. National industrial policy must also support global engagement and consensus in order to prevent silos that will defeat the adoption of IoT. It is absolutely crucial that from the beginning all involved and affected stakeholders are developing or reviewing standards jointly. While the needs of each industry have to be taken into account as the context of application for policy, high level interoperability can create both value and leverage across sectors. It is important to encourage cross sector interoperability, so as to facilitate cross sector pollination and collaboration as well as reuse of IoT outputs.

In the manufacturing industry, for example, the real-time capability in wireless standards such as WLAN and Bluetooth need to be taken into account when elaborating horizontal (non-application specific) ICT standards related to Industry 4.0 or the Industrial Internet ("advanced manufacturing, wireless digital factory"). Neglecting such industry- and application-specific requirements could lead to needless limitations in the evolution towards the future of manufacturing.

Policy makers should encourage standards development by supporting the standardization bodies where the relevant stakeholders are already active, in line with the well-established market-driven and voluntary-based standardization model. Having a number of standardization bodies involved in developing IoT relevant standards enables standards development where the technical focus fits best and where the non-technical elements, such as IPR policies, facilitate the smooth uptake and implementation of the standard.

21. *What issues, if any, regarding IoT should the Department focus on through international engagement?*

TABC supports the development of horizontal and binding commitments on all of the following principles related to the free flow of data:

- We support the cross border free flow of data, which is essential across all industries to enhance economic growth, job creation and social prosperity.
- With the objective of enhancing trust of users and certainty of companies, and thus trade in goods and services, it is essential that businesses comply with all applicable laws and regulations related to data protection and data security.
- Restrictions on data flows and associated infrastructure create risks for global business that must be recognized by governments, and their effects should be minimized by policymakers in trade agreements, legislation and regulatory proceedings. Restrictions on data flows must be consistent with the provisions set forth in GATS Article 14.

22. *Are there Internet governance issues now or in the foreseeable future specific to IoT?*

23. *Are there policies that the government should seek to promote with international partners that would be helpful in the IoT context?*

24. *What factors can impede the growth of the IoT outside the U. S. (e.g., data or service localization requirements or other barriers to trade), or otherwise constrain the ability of U.S. companies to provide those services on a global basis? How can the government help to alleviate these factors?*

Additional Issues:

25. *Are there IoT policy areas that could be appropriate for multistakeholder engagement, similar to the NTIA-run processes on privacy and cybersecurity?*

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?*

27. *How should government and the private sector collaborate to ensure that infrastructure, policy, technology, and investment are working together to best fuel IoT growth and development? Would an overarching strategy, such as those deployed in other countries, be useful in this space? If the answer is yes, what should that strategy entail?*

28. *What are any additional relevant issues not raised above, and what role, if any, should the Department of Commerce and, more generally, the federal government play in addressing them?*