UNITED STATES COUNCIL FOR INTERNATIONAL BUSINESS

June 2, 2016

The Honorable Lawrence E. Strickling
Assistant Secretary for Communications and Information
U.S. Department of Commerce
Washington, DC 20230

VIA ELECTRONIC TRANSMISSION

RE: Request for Comments – The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things (Federal Register Docket No. 160331306-6306-01)

Dear Secretary Strickling:

The U.S. Council for International Business (USCIB) is pleased to respond to the National Telecommunications and Information Administration's (NTIA) April 6, 2016 request for comments concerning the benefits, challenges and potential roles for the government in fostering the advancement of the Internet of Things (IoT). USCIB is a trade association composed of more than 300 multinational companies, law firms, and business associations from every sector of the US economy, with operations in every region of the world. In particular, USCIB Members include a broad cross-section of the leading global companies in the information and communications technology (ICT) sectors. Thus, we welcome this opportunity to offer a multi-sectoral perspective on an emerging technology that we believe potentially offers a broad range of economic, commercial, and societal benefits.

General Comments:

This Request for Comment comes at an opportune time for U.S. business, which is well-positioned to benefit from IoT technologies as well as serve as a global leader in pioneering further advancements in the development and use of IoT technologies. We offer the following general comments:

"Light Touch Regulation" -- Critical to continued innovation in IoT is a "light touch" regulatory framework. We further urge that such "light regulation" be promoted globally to ensure that the regulations themselves are interoperable and users throughout the world can benefit. It is also important to note that regulations already exist and apply to IoT with respect to privacy, data security, energy, finance, product safety and transportation. The increasing number of devices does not automatically mean that we should have new regulations. There should be evidence of real harms before considering new rules. As IoT standards and technology continue to develop, regulatory efforts should be designed to promote innovation and realize the potential value in this emerging industry.

As the Federal Trade Commission (FTC) determined in its examination of IoT, "there is great potential for innovation in this area, and that legislation aimed specifically at the IoT would be premature."

Furthermore, if there are new regulations, they will have to be harmonized with existing regulations; there will need to be further harmonization if state and federal agencies enact rules. A fragmented regulatory environment will limit innovation and growth of this industry.

Voluntary Standards -- Given the dynamic nature of IoT innovation, it is not advisable that governments impose regulations or standards aimed at realizing *technical* interoperability, since such standards likely would quickly become outdated and hamper global deployment of IoT technologies. Rather, governments should encourage business collaboration in open and global standardization efforts to develop technological best practices and voluntary standards. This is because business is in the best position to understand the potential of emerging technologies for commercial, economic, and societal benefit.

U.S. Leadership in Reducing Global Regulatory/Policy Barriers -- The U.S. government should lead efforts to reduce barriers internationally. An essential complement is to work with the International Telecommunications Union (ITU) to ensure there is sufficient spectrum, including unlicensed spectrum, to realize the benefits of IoT. The U.S. government also should tackle foreign policy barriers to IoT. Some countries are using IoT as a state-directed industrial policy aimed at leap-frogging technology development and improving their competiveness nationally, regionally, and globally. This is potentially very problematic, leading to protectionist policies that outright restrict market access of U.S. business and/or impose localization requirements on U.S. companies that wish to do business in a particular foreign market.

The Broader Digital Economy Architecture -- It is important to understand how IoT fits into the broad digital economy architecture. Care should be given to considering important "back end" technologies important to enable IoT, such as cloud computing.

Specific NTIA Questions:

NTIA poses some 28 different questions covering such topics as technology, infrastructural needs, economic impact, and policy questions. USCIB has elected to respond to the following *selected* questions, which we feel most effectively draw upon the expertise and insights of members concerning the technical, commercial, and policy implications of IoT.

General:

2. What definition(s) should we use in examining the IoT landscape and why?

The IoT is composed of a broad group of devices and technologies that include sensors incorporated into various everyday "things," along with enabling applications and cloud-based analytical platforms. Beyond this kind of broad outline, USCIB would suggest that a precise, exclusive definition of the IoT is not necessary at this point. Establishing such a definition is the first step toward regulating the group of technologies that the IoT represents, deciding which fall within and which fall outside of it. As USCIB says elsewhere, we would not support such regulations.

Technology:

6. What technological issues may hinder the development of IoT, if any: (i) interoperability; (ii) insufficient/contradictory/proprietary standards/platforms; (iii) spectrum availability and potential congestion/interference; and (iv) availability of network infrastructure.

Interoperability: IoT devices need to be quick and easy to set up and then they just need to work – first time, every time; seamlessly connecting to the network and fading into the background of our daily lives, as they perform their designed function. IoT devices need to recognize that other IoT devices may be sharing the network and avoid interference with these IoT devices.

As we discuss above, given the dynamic nature of IoT innovation, it is not advisable that governments impose regulations or standards aimed at realizing *technical* interoperability, since such standards likely would quickly become outdated and hamper global deployment of IoT technologies.

Standards and platforms: USCIB believes open standards adopted voluntarily can serve as technical building blocks for IoT interoperability as well as stimulate continued industry innovation. Multiple, competing standards and the fragmentation they cause impede development of a large-scale market which effectively creates a barrier to cost-effective entries. While open standards may be developed in both international standards bodies and industry-led global standards consortia, it is imperative that these organizations cooperate in adopting widely recognized standards so as to avoid the fragmentation problem.

Spectrum availability and potential congestion/interference: Connectivity is imperative to realize the full power of emerging technologies. In turn, spectrum may be viewed as an essential building block of IoT connectivity. Where ubiquitous and affordable high-speed broadband connections are lacking, consumers, businesses and governments lose out on the economic and societal benefits possible through IoT. In general, governments and regulators should provide a framework that incentivizes investment in broadband build-out. Specifically, we urge that spectrum licenses be granted under more harmonized terms with respect to timing, license durations, and assignment conditions.

An essential complement is to work with the International Telecommunications Union (ITU) to ensure there is sufficient globally harmonized spectrum, including unlicensed spectrum, to realize the benefits of IoT.

Availability of network infrastructure: IoT devices need communications that are robust, reliable, and secure. In particular:

- IoT devices need a communication infrastructure that has no single point of failure or has a recovery function in the case of communications failure or interruption;
- IoT devices need efficient power and possible back-up power in many instances;
- IoT devices should not place an administrative burden on the network, owner or end user.

The communications infrastructure in which IoT operates also may be weakened by insufficient attention to legacy devices. More than 85 percent of existing devices worldwide are based on

unconnected legacy systems. Solutions therefore must be developed and deployed to address connectivity and interoperability of legacy devices as an interim step to avoid replacing all existing infrastructure. This would enable the benefits that IoT and other emerging technologies to be realized in this legacy environment.

Economy:

13. What impact will the proliferation of IoT have on industrial practices, for example, advanced manufacturing, supply chains, or agriculture?

Business is using specific IoT applications to address a range of commercial needs, some of which provide direct social welfare benefits. These include fleet management, energy management, connected car, health monitoring, and cargo management. The following are examples of such applications:

- Companies have deployed IoT technology to create intelligent container fleets to improve operations with information that is delivered based on specific business needs, such as the movement of perishable or high-value cargo;
- With respect to healthcare, wireless, body-worn sensors will increasingly allow remote and continuous monitoring of patients at home by their health-care providers, thereby potentially freeing many patients from extended and expensive hospital stays. This information typically is wirelessly linked to a local monitoring hub (i.e., from a device to a router) in the patient's home, which then passes the information to the broadband network, routing it to the cloud where analytics continuously monitor a patient's status, notifying a healthcare provider of any anomalies.
- IoT shows great promise for agriculture by providing farmers with useful information such as weather reports and crop prices as well as educating them about new farming techniques. Through data generated from GPS and sensors on the field and farming equipment, and using big data analytics, farmers have been able to improve crop yields and water utilization. In addition, supported by data and analysis, farmers can benefit from precise advice about the seeds to plant, time to harvest, and expected yield[1]. Monitoring of crops and weather patterns is also used by international organizations to issue early warnings of famine or the shortages resulting from natural disasters. This can make it possible for governments to take preventive action in areas at risk[2].

Policy Issues:

15. What are the main policy issues that affect or are affected by IoT and how should the government respond?

Optimizing Opportunities -- The dynamic nature of IoT innovations naturally raises questions for policymakers about the extent to which existing policies and regulations are sufficient to facilitate continued innovation and the related economic and societal benefits, while at the same time addressing risks that may exist with some applications.

[1] http://www.aditi.com/internet-of-things-in-agriculture-case-study/
[2] https://www.itu.int/net/itunews/issues/2009/08/25.aspx

Potential risks related to privacy and security, in particular, should be appropriately considered and addressed. But at the same time, policymakers should thoughtfully consider the potential opportunity costs of overly burdensome regulations that have the effect of constraining innovation or creating unintended consequences that limit societally beneficial uses of information within or across borders.

Rather than approaching this challenge as a zero-sum exercise, USCIB believes an approach more suited to the dynamic environment of the digital economy focuses on *optimizing* the opportunity of users to leverage the benefits of IoT and other emerging technologies while maintaining a safe, secure, and trusted on-line environment.

This evaluation is not easy or without complexities, however. Overbroad definitions of "personal information" in the IoT space could prove especially problematic. With respect to concerns about protecting personal data, we feel it is important to carefully consider the nature of the information being collected and used. For example, at the business-to-business (B2B) level, many of the applications deal with non-identifiable or non-personal information, such as a jet engine providing automated reporting of its oil consumption or efficiency or operation. On the other hand, personal information will also flow over the IoT and will benefit both individual users as well as society more generally through use in healthcare research. Accordingly, it is important to pursue the "optimization approach" and develop frameworks that appropriately protect privacy while considering the context and nature of the information being collected and used through a risk-benefit analysis.

To achieve this successfully, we suggest that policymakers first defer to industry initiatives or multistakeholder proceedings that have focused, or are working, on challenges associated with a particular application of IoT technology. These initiatives can address security and privacy challenges in a more nuanced and nimble manner than government regulations. To the extent that this kind of work is not already under way to address an identified challenge, policymakers should, as a first step, convene such a group effort, rather than moving directly to regulation. Industry and multistakeholder groups have already achieved significant success in addressing the challenges posed by some of the more sensitive personal data that travels over the IoT. For example, the Consumer Technology Association has issued a set of best practices covering personal, wearable devices. And, several years ago, the Future of Privacy Forum worked with a variety of stakeholders to develop a self-regulatory regime covering consumer smart-grid data. The NIST cybersecurity framework is a similar multistakeholder success story focusing on security issues.

Evaluating security challenges posed by IoT and emerging technologies can be equally complex. The issues concern the security of the devices and the ability to hack into the device versus the data stream that emerges from the device. For the former, the concern is that the device function may be compromised. For data streams, the issue concerns the sensitivity and confidentiality of the data. Standards currently are being considered that would improve the security of devices while still permitting the interoperability that makes them useful. With respect to the security of data streams, certain mediating systems (say, a "smart house" composed of various devices connected by IoT technology) may enable individuals to control personal data collection.

The important point in evaluating privacy and security challenges posed by the IoT is use and context.

The FTC has established leadership in enforcement of strong privacy rules. For the time being, we should follow their guidance and regulatory approach to how existing privacy obligations and compliance frameworks may be used in guiding industry utilization of IoT, while urging that premature regulations be avoided.

As the FTC determined in its examination of IoT, "there is great potential for innovation in this area, and that legislation aimed specifically at the IoT would be premature."

16. How should the government address or respond to cybersecurity concerns around IoT applications? And
17. How should the government respond to privacy concerns about IoT?

A successful public policy framework must evoke consumer and industry trust through enhanced privacy and security solutions in order to motivate adoption of and participation in the marketplace for IoT and emerging technologies. Consumer notice and consent will continue to be important in ensuring appropriate protections for collection and use of personal data by IoTs. However, we caution that a strict reliance on the "consent model" may hamper some uses of IoT, particularly with implications for public safety, health-case, and other societal benefits. Many businesses rely upon the privacy principle of accountability for the appropriate collection, use, and protection of the consumer's data in a manner that takes into consideration the sensitivity of the data. We feel this affords an approach to privacy protection that safeguards the consumer, yet would continue to enable innovative uses of IoTs for various societal benefits.

Industry Self-Regulation -- The most effective privacy and security methods must be developed through industry collaboration as required for different IoT applications. Equally important is an understanding that security and privacy issues vary according to context, application, communications media used, and degree of human interaction.

Not all data processed by an IoT application is personal. Thus, when applying any privacy and security guidelines, a distinction should be made between strictly consumer applications (e.g., wearable computing, home automation), which may require more stringent risk assessment, and business applications (e.g., cargo tracking, agricultural monitoring), where the processing of personal data may be minimal or non-existent. USCIB therefore proposes that proactive industry self-regulation and collaboration with government are the most effective measures to mitigate risk yet preserve innovation.

Industry stakeholders are committed to meaningful, voluntary efforts to improve privacy and security. Thus, as set out more fully in connection to question 15, USCIB advocates the embrace of voluntary compliance and broadly accepted industry guidelines as the most productive approach to ensuring robust privacy and security standards.

19. In what ways could IoT affect and be affected by questions of economic equity? Specifically, (a) in what ways could IoT potentially help disadvantaged communities, groups, or rural communities?

IoT devices appear to enable many more efficient and unique technologies to expand. But all IoT

devices require an appropriate connection to the Internet. This connectivity often will be wireless (cellular and/or WIFI) and the connectivity will have to work with IoT devices that operate at a minimal power level. In areas where existing cellular and other communication technologies deployments are limited, IoT deployments could be challenging unless the proper "backhaul" communication is present.

To improve this situation, there should be incentives to improve rural coverage for IoT and reasonable accommodation by all local zoning jurisdictions for IoT related installations.

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?

Many IoT opportunities are global in nature. And, not surprisingly, many international organizations currently are examining via programming and solicitation of comments appropriate public policy with respect to IoT. Thus, the time is ripe for the U.S. Government to pursue bilateral or multilateral dialogues to enable a thoughtful exchange of views on policy approaches that optimize the economic and societal benefits of IoT and other emerging technologies while maintaining a secure and trusted online environment.

a. Standards and specification organizations?

As we discuss above, standards governing the technical underpinnings of IoT will play a major role in facilitating growth of the ecosystem supporting IoT. Standards will facilitate global interoperability, contribute to economies of scale, and create technical specifications to which innovators can build. Standards should be voluntary and driven by industry as they develop new products and practices that meet user needs. Their development should be undertaken in an open and inclusive manner by private-sector standard development organizations (SDOs). To reiterate an earlier point, it is imperative that these organizations cooperate in adopting widely recognized standards so as to avoid fragmentation.

We underscore that development of technical and interoperability standards should not be driven by governments, but determined by companies and markets. Government-led development of standards will be problematic as this often results in protectionist barriers. Nationally or regionally mandated IoT standards will create roadblocks to the seamless operation of a global IoT ecosystem.

Further, we strongly discourage government-led development of security-related standards. Consumer trust is critical for this industry to succeed. Companies have a built-in incentive built to protect data for IoT devices.

b. Bilateral and multilateral engagement?

Several international organizations are actively engaging on IoT public policy issues. Concerning the provision of sufficient spectrum, the ITU World Radiocommunications Conference is a natural venue in which to tackle this issue. The ITU is also active around IoT in its Telecommunications Standardization sector, where work on regulatory policy has raised concerns about expansion beyond the organization's

mandate and propensity to support government mandates that will stifle rather than promote the benefits of IoT. We encourage the Department of Commerce to pursue approaches to ensure that the ITU does not adopt policies inconsistent with the principles we have advocated throughout this document.

On the immediate horizon, the OECD Committee on Digital Economy Policy (CDEP) will devote a high-level panel to exploring "Tomorrow's Internet of Things" at its Ministerial, June 22-23, 2016 in Cancun, Mexico. This panel, composed of leading experts from all stakeholder groups, will explore many of the issues that are the focus on this RFC, including ensuring access to efficient and widespread communication infrastructures and services, as well as privacy and security, protection of consumers and more broadly addressing the potential effects on economies and societal values.

The OECD Ministerial discussion likely will produce new insights that may lend themselves to public policy "action items" warranting careful consideration by the U.S. Government to ensure a continued "light touch" approach. Equally important, the OECD intends to follow up the Ministerial discussion with an IoT-focused work-stream in the 2017-2018 period. It is imperative that the U.S. Government, in consultation and collaboration with the U.S. business community, remain actively engaged in shaping the OECD's continued focus on IoT innovative benefits and policy/regulatory challenges.

c. Industry alliances?

There are many different types of industry alliances that even now of emerging. The U.S. Government should monitor the development of such alliances and regard them as an important source of information and expertise, both technical and commercial/market oriented.

d. Other?

Push for Definitions – As we note above, USCIB does not believe it is necessary at this time to develop a precise, exclusive definition of the IoT. We are concerned that establishing such a definition would serve as the first step toward regulating the group of technologies that the IoT represents, which USCIB would not support. The U.S. Government should use its access to international organizations such as the ITU and the OECD to discourage efforts to exclusively define IoT. It should also use these organizations to push back on unnecessary national and local restrictions that could hamper innovation and prevent consumers from accessing beneficial global IoT products and services.

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

As we have discussed throughout these comments, the Commerce Department should monitor the global development of IoT and identify policies or regulations that act to impede the full potential of IoT. The goal should be to create an enabling environment that is technology neutral and market-oriented and avoids regulatory barriers and government intrusions into commerce developments and technical standards. This could, for instance, be part of the portfolio of the Department's Digital Attaches.

From a policy perspective, the U.S. Government should continue, in concert with all relevant U.S. Government agencies, to promote cross-border data flows and service provision, prohibit localization requirements, and promote workable and interoperable approaches to privacy and security. Examples of

the latter include the APEC Cross-Border Privacy Rules system and the EU-US Privacy Shield. The U.S. Government also should recognize the close nexus between IoT and 5G around spectrum.

Finally, the U.S. Government should devote more energy to creating mechanisms for intergovernmental and multistakeholder global collaboration.

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

We continue to see growing interest in the Internet Governance Forum (IGF) in exploring the economic and societal benefits of IoT along with the privacy and security-related challenges. The IGF is a valuable forum for these discussions because it enables inputs by all stakeholder groups that, to date, have been exploratory, informational, and educational in nature. This fills a crucial gap in global discourse on this subject, which, when undertaken in intergovernmental organizations, is susceptible to pressure from some governments to be "outcome oriented" or otherwise produce new regulatory prescriptions.

Multistakeholder discussion is especially valuable in addressing Internet governance issues important to the global proliferation of IoT because these tend to be targets for protectionist government policies or burdensome regulations. Examples include policies limiting cross-border data flows (ostensibly for privacy and/or security reasons) or addressing extraterritorial jurisdiction. As we discuss below, efforts to harness IoT through approaches to Internet governance that close borders not only hamper the evolution of IoT across the entire digital ecosystem, but more importantly, greatly limit the ability of the protective country to yield the benefits of this technology.

On the technical side, there may be issues regarding special use of Internet resources for IoT routing, IP addresses, and domain names, which likely benefit from multistakeholder discussion in forums such as the IGF and ICANN.

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

For regulatory considerations, governments should start with a gap analysis and an objective to introduce new government interventions only where necessary to close gaps. As we have emphasized, regulatory approaches should be "light-touch" in view of the dynamic nature of IoT innovation, the prevalence of nascent services, and the likelihood that existing policy-frameworks (e.g., privacy, security) can be used extensively for IoT.

We cannot emphasize enough that the U.S. Government, in close consultation with U.S. business, should actively oppose through bilateral, regional, and multilateral negotiations the proliferation of such protectionist devices as on mandatory technical standards, industrial policy requirements, interoperability obligations, and switching requirements, among others.

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?

Data facilities localization requirements have emerged as some of the more onerous barriers to the innovative growth of IoT. Countries as diverse as Australia, Canada, China, Germany, Indonesia, Russia and Vietnam maintain data storage requirements ostensibly to create a more secure environment governing the use of their citizens' data. Additionally, a growing number of cloud computing regulations could hamper the efficient use of and ability to scale IoT. It is imperative that the U.S. Government use every available means – trade negotiations, WTO actions, international conferences like the IGF – to forcefully advocate against the further proliferation of data localization requirements.

Other factors that serve to constrain the ability to U.S. companies to provide IoT-based products and services on a global basis and should be the focus of U.S. Government negotiation and advocacy include:

- Unnecessary regulatory requirements, such as special licenses, restrictions on use of extraterritorial numbers, requirement to register numbers and/or IP addresses;
- Classification of IoT as a traditional telecommunications service subject to burdensome and outdated regulations;
- Imposition of IoT-only policies for privacy or security; and
- Mandatory government-developed technical standards, interoperability obligations, and switching requirements

Closing Thoughts

USCIB commends NTIA for pursuing this comprehensive inquiry into a technology that holds great promise for delivering a broad-range of economic, commercial, and societal benefits. The potential for IoT will not be fully realized, however, by burdensome regulations, top-down government imposition of standards, insufficient network infrastructure, and policies that force data to remain inside national borders. The U.S. Government must use its negotiating authority to fight the proliferation of polices and regulations that would hamper the development of IoT. Concurrently, Washington must build a stronger substantive foundation to inform negotiations by becoming more actively engaged in IoT-related work-streams in organizations such as the OECD and the IGF. Equally important, dialogue with the U.S. business and other stakeholders will remain critical to effectively navigating an as-yet-to-be-charted path of innovative growth.

Thank you for your consideration.

Barbara P. Wanner
Vice President, ICT Policy