



UNITED STATES COUNCIL FOR INTERNATIONAL BUSINESS

March 6, 2017

Travis Hall
National Telecommunications and Information Administration
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. 170105023–7023–01)

Dear Mr. Hall:

The U.S. Council for International Business (USCIB) is pleased to follow up our [June 2, 2016 submission](#) to the National Telecommunications and Information Administration (NTIA) 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:

As we noted in our 2016 submission, NTIA's examination of this issue is timely and important in view of the fact that U.S. business 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.

In this regard, USCIB members support the green paper's primary themes:

1. Continued private-sector leadership in the development of IoT;
2. Government efforts to enable infrastructure availability and access;
3. The removal of regulatory barriers; and
4. Collaboration with the private sector to address potential IoT cybersecurity and privacy risks.

More generally, we encourage the Department of Commerce to articulate an overarching federal policy aimed at promoting innovation, but avoiding prescriptive regulation as well as duplicative or conflicting regulatory mandates for IoT. Ideally, the NTIA's cumulative work on IoT -- including the outcome of this latest request for public comment -- will serve as a foundation to inform policies of the Trump Administration aimed at realizing the economic and social benefits of IoT technologies.

Do Not Hamper the Benefits of IoT:

The green paper appropriately highlights the many benefits of IoT applications, including smart manufacturing, business efficiency applications, smart homes, connected vehicles, remote health care and education, and assistive technologies for disabled users. It is important that government agencies recognize and discuss the vast benefits of these various types of technology.

Importantly, these potential benefits should remain foremost in the minds of policymakers as they consider regulations affecting the development and use of IoT. We urge policymakers to remain aware of the potential of such regulations to dampen innovation or restrict the widespread economic and societal benefits of IoT technologies. As we stated in our June 2016 comments, a “light touch” regulatory framework is a critical element of an enabling environment for continued IoT innovation.

Importance of Infrastructure and Spectrum:

USCIB agrees and commends NTIA for highlighting the importance of a robust and fully deployed telecommunications infrastructure and adequate spectrum resources as another element of an enabling environment for IoT growth and innovation. In particular, we note that tower siting, pole attachment access, and spectrum availability all pose the potential to constrain the growth of IoT.

In light of the Trump Administration’s focus on rebuilding America’s infrastructure, we urge the Commerce Department to seize this opportunity to encourage the inclusion of smart technologies into large infrastructure projects that are proposed in the coming year. Specifically, we urge that smart transportation and connected car sensors be incorporated into highway development projects as a way to jump-start development of the IoT services.

Need for Cross-Agency Coordination:

USCIB was pleased to see the paper’s message underscoring the need for regulatory coordination across government agencies owing to the cross-sectoral nature of IoT. To realize such coordination, we join others in proposing that the Commerce Department convene a special inter-agency working group to ensure that regulations remain very “light touch” and do not conflict between agencies. Commerce best understands the importance of enabling the private sector to continue to take the lead in IoT innovation and is most qualified to speak authoritatively for the executive branch in streamlining government involvement.

We further encourage this interagency cooperation as the U.S. Government engages in discussions with strategic partners and essential intergovernmental organizations like the OECD about the global ramifications of IoT policy. We urge the U.S. Government to use such discussions to support cross-border data flows to facilitate IoT deployment, which along with analytics, are essential to its continued innovation.

Optimizing Privacy Needs with IoT Benefits:

The green paper correctly notes that privacy risks vary significantly across the broad range of IoT

applications, due, in part, to the varying levels of personally identifiable information that may be collected by different IoT solutions. It also rightly recognizes the threat posed by a proliferation of sector-specific privacy regulations.

We encourage the Commerce Department to use the inter-agency working group proposed above, among other means, to enable discussion of the privacy implications of IoT applications. The purpose should be to nip in the bud the impulse of numerous agencies with less privacy- and IoT-relevant expertise to impose their own, potentially inconsistent mandates.

We reiterate a point we made in our June 2016 comments, which underscored that industry stakeholders are committed to meaningful, voluntary efforts to improve privacy and security. Consumer trust is critical for this industry to succeed. Companies have a built-in incentive built to protect data for IoT devices. Thus, USCIB continues to strongly advocate the embrace of voluntary compliance and broadly accepted industry guidelines as the most productive approach to ensuring robust privacy and security standards. Private sector and multi-stakeholder initiatives will best ensure a nimble response than government regulation and can address technology flaws in a nuanced and sustainable manner. In cases where policymakers and industry agree that privacy-regulations are warranted, they should be technology neutral as the paper proposes.

Flexible Security Solutions:

USCIB is pleased to see the green paper's endorsement of flexible IoT security solutions that allow companies to respond to evolving cyber threats, noting that overly prescriptive regulatory approaches work in opposition and hamper agile response. We agree, as the paper highlights, that the NIST Cybersecurity Framework is a useful risk management tool for addressing security issues. USCIB supports the government's role of facilitating coordination and standardization on security issues, recognizing that different IoT applications present different types of security challenges.

International Standards:

USCIB cannot emphasize enough the importance of enabling a lead role for the private-sector in developing industry standards. As we stated in June 2016, 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. In this regard, we appreciate that the green paper acknowledges the protectionist effect of a government-led approach to standards development preferred by some countries and discourages this approach.

Importance of Open International Trade:

USCIB's appreciates the green paper's recognition of the importance an open trading system. From an ICT company perspective, in view of the low revenues and margins that characterize many IoT products, it is vital that companies be able to sell them as widely as possible around the world without reengineering or customizing them for particular regional or national markets. Additionally, a growing

number of trade-restrictive cloud computing regulations could hamper the efficient use of and ability to scale IoT.

Efforts to harness IoT by closing borders and/or imposing data facilities localization requirements will 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. We reiterate our June 2016 call to the U.S. government to use every available means – trade negotiations, WTO actions, international conferences like the Internet Governance Forum (IGF) – to forcefully advocate against the further proliferation of data localization requirements and trade restrictive policies and regulations.

Closing Thoughts

USCIB commends NTIA for continuing this comprehensive and inclusive inquiry into a technology that holds great promise for delivering a broad-range of economic, commercial, and societal benefits. As we emphasize above and in earlier comments, the potential for IoT will not be fully realized 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 foreign government policies and regulations that would hamper the development of IoT. At the same time, we must seize opportunities presented at home to improve domestic infrastructural requirements to ensure a healthy, innovative approach to IoT. Dialogue with the U.S. business and other stakeholders will continue to yield the most effective solutions to foster this emerging technology.

Thank you for your consideration.

A handwritten signature in cursive script that reads "Barbara P. Wanner".

Barbara P. Wanner
Vice President, ICT Policy