Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
1401 Constitution Avenue, NW
Washington, D.C. 20230

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

COMMENTS OF
USTELECOM

USTelecom[1] is pleased to comment on the notice and request for public comment (Notice) issued by the National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce (Department) regarding its green paper "Fostering the Advancement of the Internet of Things" ("Green Paper")[2] that lays out an approach and areas of engagement for the Department's possible future work on the Internet of Things (IoT).[3] Through its Notice, the Department and NTIA seek broad input from all interested stakeholders on the issues and proposed approach, current initiatives, and next steps laid out in the Green Paper.[4]

---

[1] USTelecom is the premier trade association representing service providers and suppliers for the telecommunications industry. USTelecom members provide a full array of services, including broadband, voice, data and video over wireline and wireless networks.

[2] The Department of Commerce, Internet Policy Task Force & Digital Economy Leadership Team, Green Paper: Fostering the Advancement of the Internet of Things, January 2017 (available at: https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf) (visited March 8, 2017) (*Green Paper*).

[3] See, Notice and Request for Comment, *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, 81 FR No. 66, p. 19956 April 6, 2016 (*Notice*).

[4] *Id.*, p. 19956.

I. Introduction

USTelecom appreciates the Department's discussion of the many benefits of IOT applications, which will enable greater integration of previously distinct industries, sectors, and activities. As the Department notes, IoT applications "offer the potential for industry, government, and individuals to reap benefits in terms of increased efficiency, safety, and convenience that were previously impossible."[5] These applications cover a broad range of areas, including smart manufacturing, business efficiency applications, smart homes, connected vehicles, remote health care and education, and assistive technologies for disabled users. It is helpful to have government agencies recognize and discuss the vast benefits of these various types of technology.

USTelecom has advocated at length on the role that the internet economy plays in the United States, and we are encouraged that the Department has made it a top priority to encourage growth of the digital economy and to facilitate an environment that ensures continued growth and innovation within the IoT space. It will be important for policy-makers to keep these benefits in mind when considering regulatory action with respect to the IOT. In examining particular regulatory approaches to IOT technologies, it is vital that government considers the potential for its actions to dampen innovation or restrict the widespread social benefits of IOT technologies.

It is therefore appropriate and correct that the Green Paper acknowledges that in order for the "full potential" of IoT to be realized, "the necessary infrastructure and policies must be in place."[6] As the nation moves towards the development and deployment of IoT technology, USTelecom's member companies are ideal partners to facilitate the widespread deployment and

[5] *Green Paper*, p. 4.

[6] *Id.*, p. 1.

adoption of such tools and services. USTelecom's member companies provide a full array of services to consumers, businesses and government agencies at the local, state and federal levels. These broadband-enabled suites of services range from traditional voice telephony, consumer broadband and video, as well as managed secure services for businesses and government agencies. Given that consumers and businesses alike are currently reaping the benefits that broadband networks afford, the Department and NTIA should work to ensure that appropriate policies are in place to further growth, availability and adoption of IoT devices and services.

II. The Broadband Industry's Goals are Consistent with the Principles Identified in the Green Paper Regarding Successful IoT Deployment.

The Department notes that its primary goal in issuing the Green Paper is to identify elements of an approach to foster the advancement of the IoT.[7] Consistent with that goal, the Department and NTIA proposes four principles that they say are consistent with established U.S. Government policy for emerging technologies, such as the IoT.[8] USTelecom supports adoption of the four principles identified by the Department and NTIA, which are fully consistent with the broadband industry's goals, and will be beneficial to the successful deployment of IoT devices and services. Specifically, the Green Paper proposes adoption of the following four principles in order to foster the growth of the IoT:

- The Department will lead efforts to ensure the IoT environment is inclusive and widely accessible to consumers, workers, and businesses;
- The Department will recommend policy and take action to support a stable, secure, and trustworthy IoT environment;
- The Department will advocate for and defend a globally connected, open, and interoperable IoT environment built upon industry-driven, consensus-based standards; and
- The Department will encourage IoT growth and innovation by encouraging expanding markets and reducing barriers to entry, and by convening stakeholders to address public policy challenges.

[7] *Id.*, p. 2.

[8] *Id.*.

USTelecom agrees that these principles create the necessary framework for ensuring the successful deployment and adoption of IoT technologies. The alignment of industry's shared goals with the principles proposed by the Department is discussed below.

A. Industry is Working to Ensure that Broadband Services are Widely Accessible to as Broad a Range of Consumers, Workers and Businesses.

USTelecom and its industry partners are working to ensure that broadband services are widely accessible to consumers, workers and businesses. The exponential growth in the use of the internet and the attendant explosion in internet users is no accident. This astounding growth is the result of USTelecom's member companies who have been at the leading edge of expanding access to the internet. USTelecom's annual analysis of broadband industry capital expenditures reveals that the industry invested approximately $1.5 trillion in network infrastructure over 20 years from 1996 – 2015. The wireline industry invested nearly $750 billion during this period, and in 2015 alone, the industry invested $76 billion.[9]

The Department's first principle also acknowledges the importance of broadband to workers and businesses to IoT deployment and adoption. The growth of competition for business broadband services is also great success story, where competition for such services is robust and growing. According to a competitive analysis by economists at Compass Lexecon,[10] competitive facilities are available in 95 percent of all census blocks where demand for business broadband services exists. Overall, census blocks with competitive facilities contain 99 percent of all business establishments nationwide, and areas with competitive fiber contain 92% of all

[9] USTelecom Research Brief, December 14, 2016 (available at: http://www.ustelecom.org/sites/default/files/Broadband%20Investment%20Down%20in%202015.pdf) (visited March 3, 2017).

[10] Innovate With Us website, *Revised Analysis of the FCC's Special Access Data Collection* (available at: http://innovatewithus.org/resource_posts/revised-analysis-of-the-fccs-special-access-data-collection/) (visited March 3, 2017).

business establishments nationwide.[11] In addition, cable and competitive fiber providers have invested $14 billion and $30 billion, respectively, from 2009 to 2015 to provide business broadband services – including approximately $6 billion and $9 billion, respectively, in just the last two years.[12]

Industry is poised to continue the substantial investment in the nation's broadband networks which will be crucial to the successful deployment and adoption of IoT devices and services. While significant investments have been made to build out broadband networks, more work needs to be done to ensure that all Americans have access to these vital services. In order to facilitate the investment necessary to ensure ubiquitous broadband deployment, where appropriate, government should ensure that appropriate policies are in place to further encourage robust broadband deployment.

B. The Broadband Industry Fully Supports Policies that Promote a Stable, Secure, and Trustworthy IoT Environment.

USTelecom acknowledges that well-considered and informed regulation is a key part of the evolving ecosystem, particularly as it relates to ensuring that any such ecosystem is stable, secure and trustworthy. The Department and NTIA thus should encourage regulators to work with industry to identify potential cybersecurity gaps and distribute responsibilities across the broad ecosystem of device manufactures, applications developers, network service providers and others. Regulators need not follow a traditional notice, comment and rulemaking track but instead can adopt more innovative and flexible means of collaboration with industry. The Federal Communications Commission's (FCC) Communications Security Reliability and

---

[11] *See*, USTelecom blog, *Data Confirm Widespread Competitive Investment in Business Broadband*, April 8, 2016 (available at: http://www.ustelecom.org/blog/data-confirm-widespread-competitive-investment-business-broadband) (visited March 3, 2017) (*Business Broadband Investment Blog*).

[12] *Id*.

Interoperability Council (CSRIC) serves as an important example of a regulatory agency facilitating effective multi-stakeholder engagement to identify best practices when considering new technologies and security-related threats.[13] Over a period of many years, CSRIC has been convened to bring leading technologists and thought leaders from industry, government, and academia to collaborate to address a variety of challenges, identify potential solutions, and to make recommendations that are designed to have a meaningful and positive impact for both providers and consumers.

NTIA has already demonstrated unique competencies in bringing together diverse sets of stakeholders to address complex issues associated with the rapidly evolving digital economy. Since 2010 when the Commerce Department established the Internet Policy Task Force ("Task Force") to conduct reviews on enhancing Internet privacy, improving cybersecurity, protecting intellectual property, and ensuring the global free flow of information, the Task Force and the agency have taken on numerous topics, expanding their role in building multi-stakeholder consensus policies around emerging technologies. Most recently, issues have included privacy and facial recognition technologies, smart city infrastructure and policy, unmanned aircraft systems, and vulnerability disclosures, to name a few. Because the Commerce Department can leverage the expertise across six agencies under its domain, including the Economic and Statistics Administration, the International Trade Administration, the National Institute of Standards and Technologies (NIST), NTIA, the Office of the Secretary, and the U.S. Patent and Trademark Office, it is uniquely qualified to bring diverse talent and knowledge across government and industry.

[13] *See*, FCC website, Communications Security, Reliability and Interoperability Council (available at: https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-1) (visited March 8, 2017).

One example of how such multi-stakeholder engagement can mitigate or negate the need for prescriptive regulation in this arena is evidenced by NIST's Framework for Cybersecurity-Physical Systems.[14] The report followed an almost two year effort by industry, academia, and government participants who examined how to standardize cyber-physical systems development to ensure trustworthiness of emerging technologies and efforts to build in security and privacy by design. The first stage of this effort, along with the current NTIA inquiry, can serve as a strong foundation for constructing IoT security standards.

USTelecom endorses the Department's support of a flexible cybersecurity framework that can be scaled to organizations' different needs, allowing them to take into account their particular business models, assets, and other variables.[15] As noted by the Department, such a structure "enables organizations to adapt to an ever-changing, dynamic environment, which is critical for IoT technologies."[16] The Department appropriately references the NIST Cybersecurity Framework as a useful risk management tool for addressing security issues.[17]

USTelecom supports the government's role of facilitating coordination and standardization on security issues, recognizing that different IoT applications present different types of security challenges. True security and trustworthiness in the IoT ecosystem, however, will be reliant on all industry stakeholders ensuring the implementation and adoption of such cybersecurity mechanisms.

C. The Broadband Industry Supports Efforts to Promote a Globally Connected, Open, and Interoperable IoT Environment Built Upon Industry-Driven, Consensus-Based Standards.

---

[14] *See*, NIST website, *Cyber Physical Systems Public Working Group, Framework for Cyber-Physical Systems, Release 1.0*, May, 2016 (available at: https://pages.nist.gov/cpspwg/) (visited March 8, 2017).

[15] *Green Paper*, pp. 25 – 27.

[16] *Id.*, p. 27.

[17] *Id.*, pp. 26 – 27.

USTelecom strongly supports the principle envisioning an affirmative role for the Department to advocate for and defend a globally connected, open, and interoperable IoT environment built upon industry-driven, consensus-based standards. The Department has a crucial role to play in advocating for international policies that reduce and avoid unnecessary burdens on global IoT applications.

Government action on IoT must also keep in mind the vital importance of cross-border data flows, and should not restrict the legitimate movement of data across national borders. In an increasingly digital global economy, ensuring that data can flow across borders and be stored without facilities localization requirements has been a priority for U.S. businesses of all types, from manufacturing to telecommunications and countless other services. In the IoT sphere, the Department should work to ensure that this policy is broadly accepted and adopted.

In addition, USTelecom appreciates the Green Paper's strong support for continuing the longstanding government policy favoring private-sector development of industry standards. The Department should therefore encourage international governments to promote the development of standards and operating frameworks for IoT that are developed through industry led, voluntary processes. Such an approach appropriately recognizes the hazards that can arise from protectionist efforts of other countries' government-led approach to standards development.

D. The Department and NTIA Should Encourage Expanding Markets and Reducing Barriers to Entry, and by Convening Stakeholders to Address Public Policy Challenges.

Consistent with the broadband deployment efforts of industry discussed above, USTelecom supports efforts by the Department to expand markets and reduce barriers to entry. Regulatory obligations often times present unique challenges and impose significant barriers to the efficient and speedy deployment of broadband services. Elimination of such regulatory barriers will result in the directing of additional resources toward the high-speed networks of

tomorrow, heralding an era of further increases in competition in the market for truly high-speed broadband services. Such a result will further the Department's goal of fostering the advancement of the IoT.

Given the enormous breadth and jurisdiction of federal government agencies, it is understandable how regulatory barriers frequently arise that impede the deployment of broadband throughout the country, thereby hampering the deployment of IoT devices and services. USTelecom has previously identified areas where the Department can take steps to remove these barriers, thereby speeding broadband deployment.[18] The Department should look to addressing these barriers as it moves forward with implementation of favorable IoT policies.

USTelecom also supports the Department's principle to convene stakeholders to address public policy challenges. In recent years, U.S. Government policy in an area of critical impact on IoT, namely cybersecurity, has been predicated on the assumption that a partnership between industry and government is superior to any prescriptive compliance regime, which, by its nature, would lack flexibility to respond promptly to new threats and potentially undermine security by providing the playbook for bad actors to exploit.[19] Following a year-long effort by NTIA's sister agency NIST to develop the Cybersecurity Framework, it is now widely acknowledged that a voluntary and non-prescriptive risk management approach based on a common security taxonomy is more likely to produce sought-after results than reliance on traditional regulatory mandates. IoT will no doubt create a larger attack surface for bad actors interested in disrupting services or exploiting weaknesses for financial or other benefits. For these and other reasons, it is

[18] *See*, Comments of USTelecom to the Department of Commerce and NTIA, *Broadband Opportunity Council Notice and Request for Comment*, Docket No. 1540414365–5365–01 (submitted June 10, 2015) (*USTelecom Broadband Council Comments*).

[19] *See e.g.*, Executive Order, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013 (available at: https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity) (visited March 8, 2017).

essential that the approach taken by the U.S. Government is thoughtful and based on processes that have been proven to be successful.

III. Wireline Broadband Networks Are Integral to the Successful Deployment of the Internet of Things.

In light of the tremendous projected growth of IoT devices and services, the Department and NTIA should not lose sight of the core role that wired networks will play in providing the backbone to accommodate these projected surges in data traffic. Indeed, the Green Paper acknowledges that the "sheer magnitude of IoT devices connected will impose significant challenges for the current infrastructure," to include those relating to capacity and resiliency.[20]

The Green Paper acknowledges that the number of connected IoT devices is project to grow rapidly in coming years. According to Cisco, it is estimated that between the years of 2015 and 2020, the number of connected devices in the United States will nearly double from 2.3 billion to 4.1 billion; and globally connected devices will increase from 16 billion to 26 billion over the same period.[21] Other forecasts project even more robust development, with estimates that the IoT market will grow from an installed base of 15.4 billion devices in 2015 to 30.7 billion devices in 2020 and 75.4 billion in 2025.[22] Moreover, McKinsey Global Institute has projected that, by 2025, the overall impact of these devices on the global economy will be between $4 trillion and $11 trillion.

As an illustrative comparison, nearly all mobile data traffic currently rides over wired

---

[20] *Green Paper*, p. 4.

[21] *Id*.

[22] Forbes, Louis Columbus, *Roundup Of Internet Of Things Forecasts And Market Estimates, 2016*, (available at: https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#132819f1292d) (visited March 3, 2017).

networks, whether via Wi-Fi, which is merely a short-range extension of a wired network, or via the longer-range wired backhaul connections that link cell towers to broader voice and data networks.[23] Globally, 60 percent of traffic from mobile devices was off-loaded onto wired networks in 2016, and that will grow to 63 percent in 2021, according to the VNI mobile forecast. In the United States, 64 percent of traffic from mobile devices was off-loaded onto wired networks in 2016, and that will grow to 70 percent in 2021. Given the integral role of wired networks in the mobile space, it is inevitable that they will likewise play a similarly crucial role in the IoT sphere.

As noted previously, wired network providers already invest significant amounts of capital to accommodate all types of traffic growth, including continually expanding capacity for mobile network off-load. Additional investment will be necessary by these same wired network providers to ensure appropriate capacity for supporting IoT services.

IV. The Department and NTIA Should Develop and Support a Policy Framework that Incentivizes Investment in Broadband Infrastructure.

The IoT solution will depend upon both public and private connectivity, which will require deployment of robust broadband infrastructure for the purpose of supporting IoT devices and services. Ongoing infrastructure investment is essential to meeting the nation's broadband deployment goals, and ensuring the success of IoT technologies and services. Regulatory decisions and other government actions that make it harder or less practical to invest, run counter to the Department's goal of encouraging the deployment and adoption of IoT technologies.

---

[23] *See*, USTelecom website, *Mobile Growth Relies on Wired Network Investment*, February 13, 2017 (available at: http://www.ustelecom.org/blog/mobile-growth-relies-wired-network-investment) (visited March 8, 2017).

As such, federal policies that incentivize ubiquitous broadband connectivity will be an important factor in achieving the many benefits of widely deployed IoT technologies. USTelecom's member companies, many of which are small businesses, annually invest tens of billions of dollars in America deploying, improving and maintaining communications networks that make available voice, video and broadband services to virtually every home and business in this country. There are few if any industries that are more committed to supporting American economic growth through private investment in their essential infrastructure.

As noted in our comments submitted last year to the Broadband Opportunity Council (Council), USTelecom's members have experienced firsthand barriers to broadband infrastructure deployment.[24] Then, as now, USTelecom encourages the Department and NTIA to take concrete steps to create and sustain a regulatory environment that provides clear incentives for investment, including the removal of barriers and the promotion of facilities-based competition. The Department and NTIA should work with both Executive branch agencies and independent agencies to remove regulatory barriers to broadband adoption.[25] By removing such barriers, NTIA can ensure that the robust broadband networks essential to the success of the IoT are deployed throughout the country. NTIA's previous efforts associated with the implementation of the Broadband Technology Opportunities Program (BTOP), should

[24] *See*, *USTelecom Broadband Council Comments*.

[25] For example, in 2014, USTelecom filed with the FCC a petition for forbearance from various outdated regulatory requirements applicable only to incumbent local exchange carriers (ILECs). *See*, Petition of USTelecom for Forbearance Pursuant to 47 U.S.C. § 160(c) from Enforcement of Obsolete ILEC Legacy Regulations That Inhibit Deployment of Next-Generation Networks, WC Docket No. 14-192 (filed Oct. 6, 2014). As USTelecom explained in its Forbearance Petition, unlike most broadband providers – including cable, wireless, and competitive fiber providers – ILECs are not free to focus their expenditures on next-generation networks designed to deliver the higher-speed broadband services customers increasingly crave; instead they "must direct a substantial portion of their expenditures to maintaining legacy networks and fulfilling regulatory mandates whose costs far exceed any benefits." *Id.*, at 3.

provide the agency with an appreciation for the important role to be played by broadband networks in the IoT space.

V. The Department and NTIA Should Encourage Cross-Agency Coordination on IoT Issues.

The Green Paper correctly emphasizes that regulatory coordination across government agencies would be helpful, due to the cross-sector nature of IoT.[26] The Department appears ideally suited to look out for the interests of U.S. business in such a cross-agency group. It well understands many of the considerations that are important to business and can speak authoritatively for the administration in seeking to streamline government involvement and allow the private sector to address issues in the first instance.

In its effort to define "next steps," the Department proposes to "coordinate with the private sector, as well as federal, state, and local government partners, to ensure the infrastructure to support IoT continues to expand, that access to infrastructure is inclusive and affordable, and that the infrastructure remains innovative, open, secure, interoperable, and stable."[27] USTelecom applauds the Department for identifying these laudable and necessary goals, and just as important, for setting this agenda in the context of immediate engagement. The rapidly accelerating deployment of IoT enabled devices and applications and their associated cybersecurity risks require that government and industry work immediately and collaboratively to build a comprehensive policy architecture that is sufficiently flexible and adaptive to withstand the pending onslaught of new devices.

---

[26] *Green Paper*, p. 2 (stating that "The Department heard a strong message from the submitted comments that coordination among U.S. Government partners would be helpful, because of the complex, interdisciplinary, cross-sector nature of IoT. A federal coordination structure for these issues may also be helpful when working with international and private sector partners.").

[27] *Id.*, p. 23.

USTelecom believes that the Department and two of its primary divisions NTIA and NIST, are in a unique position to facilitate this process and we encourage close collaboration with the Department of Homeland Security as well. Each of these entities brings critical perspectives, capabilities and resources that are essential in rationalizing government engagement when examining a field that touches on virtually every aspect of our digital economy and our nation's national security. While it is difficult to quantify the high cost of policy fragmentation and splintering engagements across the government landscape, there can be no question that a well-coordinated and facilitated process involving all relevant stakeholders focused on clearly identified outcomes is the most cost-efficient path towards making progress in this area.

USTelecom notes that IoT has several dimensions that require a different set of guidelines, standards and processes. It is evident that traditional critical infrastructure sectors like telecommunications and more traditional utilities are becoming increasingly reliant on sophisticated and dispersed sensor technologies that interconnect with key control systems. These devices provide operational efficiencies and information resources that are not only changing the ways services are delivered, but directly impact the underlying economics of their industries. DHS leads the Federal government's efforts to secure our nation's critical infrastructure and works with owners and operators of 16 critical infrastructure sectors to prepare for, prevent, mitigate, and respond to threats. It is in this capacity USTelecom believes that important considerations related to the use of IoT and the potential impact it can have on sector resiliency and emergency response comes into play. Any overarching government initiative in this space should be conducted in coordination with the Department.[28]

[28] *See*, Department of Homeland Security website, *Executive Order (EO) 13636 Improving*

We also maintain that such an initiative falls squarely within the broad mission of the Department of Commerce where the experience, expertise and resources needed to manage this engagement reside. NIST, through its extensive engagement in this field including, among other things, the development of the Cybersecurity Framework,[29] NIST Cyber Physical Systems,[30] and IOT Enabled Smart Cities, is uniquely qualified to conduct a broad inquiry into the issues raised in these comments.[31] It is worth noting that while the NIST Cybersecurity Framework focused largely on risk management processes in cybersecurity, it could very easily be used as a foundation for addressing risk associated with IoT-related devices and infrastructure. The other NIST organization that brings a set of relevant and unique skills is the National Telecommunications and Information Administration (NTIA). NTIA has had tremendous success in bringing together a wide array of technology stakeholders from government, industry, academia, and the research community.

This experience in facilitating discussions on complex organizational, process, and technology considerations will be an essential aspect of a successful multi-stakeholder initiative. We take note of the recent success involving the Vulnerabilities Disclosure project[32] and the

---

Critical Infrastructure Cybersecurity Fact Sheet, (available at: https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf) (visited March 8, 2017).

[29] *See*, NIST Cybersecurity Framework website, (available at: https://www.nist.gov/cyberframework) (visited March 8, 2017).

[30] *See*, NIST website, *Cyber-Physical Systems, CPS Public Working Group* (available at: https://www.nist.gov/el/cyber-physical-systems/cps-public-working-group-pwg) (visited March 8, 2017).

[31] *See*, NIST website, *Cyber-Physical Systems, IES Cities Architecture* (available at: https://www.nist.gov/el/cyber-physical-systems/ies-cities-architecture) (visited March 8, 2017).

[32] *See*, NTIA website, *Improving Cybersecurity Through Enhanced Vulnerability Disclosure* (available at: https://www.ntia.doc.gov/blog/2016/improving-cybersecurity-through-enhanced-vulnerability-disclosure) (visited March 8, 2017).

current work in the Multi-stakeholder Process; IoT Security Upgradability and Patching[33] as evidence of NTIA's capabilities and on-going contributions in this area. Simply put, an effort of this magnitude supported by DHS, NIST and NTIA is likely to have the greatest probability of success and we hope that the Department will consider such a cross-agency initiative.

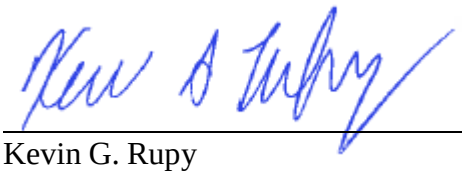
VI. Conclusion

USTelecom appreciates this opportunity to participate in the Department's and NTIA's proceeding on the IoT. The four principles identified by the Department and NTIA align with industry's shared goals, and will create the necessary framework for ensuring the successful deployment and adoption of IoT technologies. USTelecom encourages the adoption of federal policies that incentivize ubiquitous broadband connectivity, as well as regulatory coordination across government agencies, due to the cross-sector nature of IoT.

Respectfully submitted,

USTELECOM

By:



Kevin G. Rupy
Robert Mayer

Its Attorneys
607 14th Street, NW, Suite 400
Washington, DC 20005
(202) 326-7300

March 13, 2017

[33] See, NTIA website, *Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching* (available at: https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security) (visited March 8, 2017).