U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

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

COMMENTS OF THE NCTA – THE INTERNET & TELEVISION ASSOCIATION

William A. Check, Ph.D.
Senior Vice President, Science & Technology
and Chief Technology Officer

Matt Tooley
Vice President,
Broadband Technology

Rick Chessen
Loretta Polk
NCTA – The Internet & Television Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222- 2445

March 13, 2017

TABLE OF CONTENTS

U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

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

COMMENTS OF THE NCTA – THE INTERNET & TELEVISION ASSOCIATION

The NCTA – The Internet & Television Association ("NCTA")[1] hereby submits its comments on the above-captioned Notice and Request for Public Comment ("Notice").[2]

INTRODUCTION

In its Notice, NTIA requests comment on the Department of Commerce's Internet Policy Task Force ("Department") green paper on "Fostering the Advancement of the Internet of Things." The paper identifies key issues in the deployment of Internet of Things ("IoT") technologies, highlights potential benefits and challenges, and discusses the role, if any, of the federal government in this evolving landscape.[3] As NCTA noted in its initial comments in this proceeding, this is a matter of significant interest to cable broadband service providers, whose

---

1 NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving more than 90 percent of the nation's cable television households and more than 200 cable program networks. The cable industry is the nation's largest provider of broadband service after investing over $245 billion since 1996 to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to approximately 30 million customers.

2 NAT'L TELECOMMS. AND INFO. ADM., *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, Notice, Request for Public Comment, 82 Fed. Reg. 4313 (rel. Jan. 13, 2017).

3 DEP'T OF COM., Internet Policy Task Force & Digital Economy Leadership Team, *Fostering the Advancement of the Internet of Things*, at 17 (Jan. 2017), https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf ("Green Paper").

investment in, deployment and management of, Internet facilities and technologies has fueled the rapid growth and transformation of the Internet over the past several decades.[4]

As policymakers begin to examine the consumer benefits and challenges of IoT, the green paper advocates four broad areas of government engagement: 1) fostering physical and spectrum-related infrastructure assets to support IoT growth; 2) encouraging coordination and collaboration and balanced policy through multistakeholder engagement; 3) promoting open standards to support global interoperability and technology advancement; and 4) promoting IoT advancement through Department of Commerce usage of IoT technologies, as well as sharing benefits and opportunities of IoT with foreign partners.[5]

The Notice asks whether this approach and the current initiatives and next steps spelled out in the green paper are comprehensive enough and what, if any, additional steps should be taken to advance IoT. NCTA strongly supports the green paper's overall approach. Rather than intervening prematurely in the nascent, rapidly changing IoT marketplace, the green paper observes *and reaffirms* that the role of government is to establish and support an environment that promotes the development and growth of emerging technologies by "[e]ncouraging private sector leadership in technology and standards development, and using a multistakeholder approach to policy making."[6] It posits that coordination among federal government partner agencies is important because of "the complex, interdisciplinary, cross-sector nature of IoT."[7]

---

4 Comments of the National Cable & Telecommunications Association, Dkt. No. 170105023-7023-01, at 3 (June 2, 2016).

5 *See generally* Green Paper.

6 *Id.* at 2.

7 *Id.*

And it sets forth a path to help ensure that the IoT marketplace evolves in a way that benefits consumers, competition, and innovation.[8]

In response to the Notice, NCTA emphasizes several areas below that warrant particular attention in the next phase of the government's engagement in this area.[9]

DISCUSSION

I. UNLICENSED SPECTRUM IS CRITICAL TO IoT INNOVATION

As the Department notes in the green paper, "[w]ireless technologies are likely to play a significant role in supporting many of the increasing numbers of connected devices being developed by IoT manufacturers."[10] And IoT innovators will need access to spectrum – especially *unlicensed* spectrum – to support growing demand for IoT technologies.[11] Although prescriptive government regulation could stifle the nascent IoT industry, NTIA and the FCC will still have an essential role to play in making available adequate unlicensed spectrum for IoT use.

A myriad of early IoT applications, including home security and automation, wearables like fitness trackers and smart watches, and smart city deployments, industrial and retail inventory tracking – rely on unlicensed technologies like Wi-Fi, Bluetooth, Low Power Wide Area Networks, and RFID.[12] Recent IoT advances, including low power, wide-area networking for applications such as utility metering, environmental monitoring (*e.g.*, temperature, pollution, noise), and asset tracking, also rely on unlicensed spectrum.[13] Given the low barriers to entry for

---

8 *Id.* at 3.

9 *Id.*

10 *Id.* at 15.

11 *See id.* at 17-18.

12 *See* Cisco, *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021*, at 16-17 (2017), http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf.

13 *See* Semtech, *What is LoRa?*, http://www.semtech.com/wireless-rf/internet-of-things/what-is-lora/ (last viewed Feb. 22, 2017).

use of unlicensed bands – which require only that users abide by certain technical rules without the need to invest billions of dollars for spectrum at auction – it is no wonder that these bands have become mainstays for IoT innovation.

Innovative technologies that rely on unlicensed spectrum generate billions of dollars in economic value for the U.S. economy every year and new IoT devices and applications will likely generate billions of dollars more. One study concludes that unlicensed spectrum generated $222 billion in value for the U.S. economy and contributed $6.7 billion to U.S. Gross Domestic Product in 2013.[14] IoT forms an important part of that value creation and will continue to do so as the industry grows. IDC predicts that global IoT revenue will reach more than $7 billion by 2020, up from approximately $2.7 billion in 2015.[15]

Adequate unlicensed spectrum resources, however, are critical to ensuring that IoT reaches its potential. Existing unlicensed bands are quickly becoming congested as demand for unlicensed devices and services skyrockets. Congestion in the 2.4 GHz band has reached a point at which Apple and Cisco conclude that the band "is not considered as best suiting the needs for business . . . applications."[16] Congestion in unlicensed bands will only become more acute as demand grows for IoT. Ericsson forecasts that in 2018, IoT devices will surpass mobile phones as the largest category of connected mobile devices.[17] By 2021, Ericsson estimates that of 28

---

[14] Raul Katz, *Assessment of the Economic Value of Unlicensed Spectrum in the United States*, Final Report, at 8 (Feb. 2014), http://www.wififorward.org/wp-content/uploads/2014/01/Value-of-Unlicensed-Spectrum-to-the-US-Economy-Full-Report.pdf.

[15] IDC, *IDC Market in a Minute: Internet of Things* (2016), http://www.idc.com/downloads/idc_market_in_a_minute_iot_infographic.pdf.

[16] Cisco, *Enterprise Best Practices for iOS Devices on Cisco Wireless LAN*, at 4 (rev. Nov. 2016), http://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/technotes/8-3/Enterprise_Best_Practices_for_Apple_Devices_on_Cisco_Wireless_LAN.pdf.

[17] Ericsson, *Ericsson Mobility Report – On the Pulse of the Networked Society*, at 10 (June 2016), https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf.

billion connected devices, nearly 16 billion will be related to IoT, and the vast majority of those 16 billion will rely on unlicensed spectrum.[18]

NTIA and the FCC will play a leading role in making sufficient unlicensed frequencies available for IoT and both agencies have taken important steps in the right direction. NTIA's recent report, *Quantitative Assessments of Spectrum Usage*, provides information on government use of five spectrum bands as "an intermediate step" to help NTIA "determine the extent to which frequencies assigned to these agencies could be further evaluated for sharing with commercial users."[19] For its part, the FCC issued an order in July 2014 designating the 64-71 GHz millimeter wave band for unlicensed use.[20] As the FCC noted in its Order, millimeter wave bands such as this one will be critical to the development of 5G, including innovative IoT applications.[21] The FCC has also taken preliminary steps toward authorizing shared unlicensed use of the 5.9 GHz band.[22] The 5.9 GHz band is the single best near-term opportunity to make additional unlicensed spectrum available to relieve congestion and foster the development of the next generation of unlicensed innovations, including IoT.[23]

In light of the foregoing, we support the green paper's recognition that ensuring IoT reaches its full potential requires continued focus on the deployment of and investment in

---

[18] *C.f. id.* at 10-11 (predicting 16 billion IoT devices by 2021, only 1.5 billion of which will have cellular connectivity).

[19] U.S. DEP'T OF COM., *Quantitative Assessments of Spectrum Usage*, at vi (Nov. 2016), https://www.ntia.doc.gov/files/ntia/publications/ntia_quant_assessment_report-no_appendices.pdf.

[20] *Use of Spectrum Bands Above 24 GHz for Mobile Radio Services, et al.*, Report and Order and Further Notice of Proposed Rulemaking, 31 FCC Rcd. 8014, 8062 ¶ 125 (2016).

[21] *Id.* at 8021 ¶ 9, 8082 ¶ 185.

[22] *See, e.g.*, *The Comm'n Seeks to Update and Refresh the Record in the "Unlicensed Nat'l Info. Infrastructure (U-NII) Devices in the 5 GHz Band" Proceeding*, Public Notice, 31 FCC Rcd. 6130, 6133 (2016).

[23] *See* Letter from Christopher Szymanski, Director – Product Marketing and Gov't Relations, Broadcom, Rick Chessen, Senior VP, Law & Regulatory Policy, NCTA, and John Kuzin, Vice President & Regulatory Counsel, Qualcomm to Marlene H. Dortch, Secretary, FCC, ET Docket No. 13-49 (filed Feb. 3, 2017).

wireless connectivity, spectrum availability, and standards development. NTIA proposes sensible next steps, notably coordinating with the private sector and federal partners to ensure the infrastructure to support IoT continues to expand and continuing to innovate in spectrum management to increase access to spectrum to facilitate IoT growth and advancement.

II. IoT SECURITY EFFORTS SHOULD INCLUDE CONTINUING SOFTWARE UPDATES, AND DEVICE AUTHENTICATION AND AUTHORIZATION

In the cybersecurity policy area, the Department of Commerce plans to continue to bring private sector experts together with policymakers to define security principles for IoT, facilitate IoT security framework development by sector and application, and encourage the implementation of best practices and/or minimum standards.[24] It intends to further promote "the IoT environment that encourages risk-based approaches, security by design, and the ability to fix or 'patch' insecure software and devices." It will also, among other things, "promote use of strong encryption in IoT services and products" and collaborate with industry to educate consumers on such issues as "how to limit risks associated with unsecured connected devices (*e.g.*, by changing default passwords, using password-protected home Wi-Fi networks, and employing virtual private networks."[25] NCTA fully endorses these important goals.

In particular, as NCTA noted in our initial comments, cybersecurity depends upon continuing secure and automated software updates to Internet-connected computers and devices, including IoT devices, in order to keep up with and thwart cyber attacks. As the Broadband Internet Technical Advisory Group (BITAG) observed in its November 2016 report on IoT security:

> Some IoT devices ship "from the factory" with software that either is outdated or becomes outdated over time. Other IoT devices may ship with more current software, but

[24] Green Paper at 2, 41.

[25] *Id.* at 41.

> vulnerabilities may be discovered in the future. Vulnerabilities that are discovered throughout a device's lifespan may make a device less secure over time unless it has a mechanism to subsequently update its software.[26]

The green paper recognizes that "[t]he lifecycle of a device lasts beyond the development process and will vary greatly depending on the device, from short periods to many years."[27] And it further notes that software patching capability is critical as unpatched IoT devices create security vulnerabilities and manufacturers of connected devices often lack an effective update and upgrade path once installed. The BITAG Report recommended that manufacturers in the IoT supply chain should play their part in addressing IoT security and privacy issues to prevent introduction of malware during the manufacturing process; support IoT devices for entire lifespan; and provide consumers with clear methods to determine who to contact for support about software vulnerabilities and related issues.[28] NCTA supports efforts to foster this security chain for the IoT.

We are particularly pleased to see NTIA's attention to the importance of addressing the threat posed by orphan devices – devices no longer supported by their manufacturers. The paper states that "[d]evices that consumers continue to use to connect to the Internet should be updated and protected even if device manufacturers discontinue them."[29] This is the right objective, and,

---

[26] Broadband Internet Technical Advisory Group ("BITAG"), *Internet of Things (IoT) Security and Privacy Recommendations*, BITAG Technical Working Group Report, at 4 (Nov. 2016), http://www.bitag.org/documents/Press_Release_-_Announcing_Publication_of_BITAG_Report_on_IoT_Security_and_Privacy_Recommendations.pdf ("BITAG Report"). BITAG is a non-profit, multistakeholder organization which brings engineers and technologists together to develop consensus on broadband network management practices and related technical issues that can affect users' Internet experience, including the impact to and from applications, content and devices.

[27] Green Paper 28.

[28] BITAG Report at 7-8.

[29] Green Paper at 41.

to this end, we endorse developing a mechanism to ensure that devices do not function without the software updates needed to ensure security.

In addition to the areas of study for cybersecurity outlined in the green paper, it is important that the multi-stakeholder process also focus on insecure communications in IoT devices in three other areas that the paper does not address. First, a key element to cybersecurity is being able to identify the user and in the case of IoT identify the device. IoT devices should incorporate an attestable, immutable, and unique identifier for each device to aid in the lifecycle and management for the device. Second, in conjunction with being able to identify the device, it is also important for the devices to support a method for authentication and authorization, whether it is local communications by the end-user or device or whether it is via remote communications such as a software update from the manufacturer. In both contexts, authentication requires a method or process (*e.g.* strong passwords, etc.) to validate the person or machine that is trying to communicate with the device. And it is equally important that once the communications has been authenticated, the person or device is authorized, *i.e.* has the requisite permission to perform the requested operation. Third, it is important to promote efforts to address data confidentiality – how data is treated at rest in the device to ensure that it does not leak or be used inappropriately. This is in addition to encrypting data in transit and protecting customer privacy in general.

Another security area that the green paper does not address is the growing problem of overall manageability of IoT devices for end-users. This issue arises, for example, where the end-user has many IoT devices integrated into his or her home (*i.e.*, thermostat, garage door opener, door bell, sprinkler system, security cameras, etc.) and the user moves to a new home. How does the end-user keep an inventory of all the devices, manage the credentials and

more importantly revoke the credentials on all the installed devices to ensure that the new owner does not inadvertently use the previous owners credentials.

We are encouraged that the multistakeholder process will be able to tackle these matters. This process envisions fostering a market offering more devices and systems that support security upgrades, best practices for patching, vulnerability notification, and control of data retention for IoT products.

III. INDUSTRY-LED STANDARDS-SETTING IS CRITICAL TO IoT REACHING ITS FULL POTENTIAL

The Department agrees with initial commenters that "an industry-led, bottom-up, consensus-based approach to standards development is necessary to realize the benefits of the technology."[30] And it asserts that a wide range of standards addressing different aspects of IoT applications – technology, connectivity, interoperability, functionality, security, usability, etc. – will be needed. It intends to monitor IoT technology developments and applications and contribute to research and development involving those technologies.

NCTA's member companies have a strong interest in standards development through various multistakeholder initiatives. Although IoT is developing quickly, it is still in its infancy. Many applications are purely conceptual or have not been conceived yet, and will not be realized until appropriate interoperability standards have been developed to allow the IoT to grow to scale and reach its full potential. Developing standards that enable integration and interoperability of IoT devices, network and data systems, business processes, and management personnel will be important to realizing the promise of the IoT. The specifications of IoT devices differ significantly – from processing capacity, memory, and size to functional sophistication.

[30] Green Paper at 47.

Integrating big data analytics algorithms and capabilities with IoT devices will be critical to transforming raw data into useful, actionable intelligence to serve consumers. We anticipate that IoT standards setting will be more complex and time consuming than other standards-setting processes, and standards and middleware will take several years to develop.

NIST recently took steps to address the lack of a baseline set of analytic and descriptive set building blocks regarding IoT security and operational issues.[31] It published a report providing an underlying and foundational science for IoT-based technologies in order to help researchers better understand IoT and its security challenges and better communicate with one another.[32] In addition, the NIST Framework for Cyber Physical Systems presents a framework of standards to help developers of "smart" systems build cybersecurity and privacy into their designs.[33] NIST's work in developing a common language for addressing IoT issues across the Internet ecosystem – including product developers, security specialists, app designers, network providers, government agencies, and academia – will be very useful to future standards work.

While standards-setting is a daunting challenge, cable companies are well-positioned to join other stakeholders in helping to develop standards given industry experience and capabilities in addressing security issues in a consumer-facing manner. NCTA's Cybersecurity Working Group, which is comprised of a wide cross-section of cable system operators provides a forum for operators to discuss cybersecurity issues and share information and best practices. It recently

---

[31] *See* NAT'L INST. OF STANDARDS AND TECH., *Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* (Nov. 2016), http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf.

[32] *See* NAT'L INST. OF STANDARDS AND TECH., *Networks of "Things"*, NIST Special Publication 800-183 (July 2016), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf.

[33] *See* NAT'L INST. OF STANDARDS AND TECH., *Framework for Improving Critical Infrastructure Cybersecurity*, (Feb. 12, 2017), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

created a subgroup to focus solely on IoT security. The cable industry's research and development consortium, CableLabs, is devoting substantial resources to cybersecurity research and innovation to support the continued growth in broadband services and products. It has a long history of securing devices within and beyond the cable industry, using a public key infrastructure (PKI).[34] Leveraging this expertise, CableLabs is working to enhance IoT security through standards bodies and industry working groups including the Open Connectivity Foundation in such areas as device identity, authentication, authorization, delivery of software updates and managing the complexities of device life cycles. Cable system operators also participate in other standards groups addressing IoT security, including the Society of Cable Telecommunications Engineers (SCTE), Institute of Electrical and Electronic Engineers (IEEE), and the Internet Engineering Task Force (IETF). The industry will continue to participate and promote such IoT efforts.

NCTA encourages the Department to continue to monitor international standards development efforts, particularly the scope and potential for duplication of such work with other standards work.

[34] Since 1999, CableLabs has managed the specifications that require embedding digital certificates into cable devices, including cable modems, VoIP terminals, CableCARDs, and Uni-Directional Cable Products (UDCPs), at the time of manufacture. The certificates provide the basis for data confidentiality, content integrity, and hardware authentication. In addition, CableLabs, through its subsidiary – "Kyrio," manages the PKI that issues the embedded digital certificates to cable device manufacturers. *See* http://www.kyrio.com/security/. Through Kyrio, CableLabs also provides electric utilities with a managed PKI service that ensures device security for "smart grid" and specifically, automated demand response. *See* http://www.openadr.org/cyber-security. Kyrio provides a similar managed PKI service to the Wi-Fi Alliance to secure "Passpoint" certified hotspots. *See* http://www.wi-fi.org/certification/certificate-authority-vendors. To date, Kyrio has issued over 400 million device certificates off of the CableLabs PKI. *See* http://www.kyrio.com/security/.

IV. IoT PRIVACY POLICY SHOULD SEEK TO BALANCE THE TWIN OBJECTIVES OF PROTECTING CONSUMERS WHILE PROMOTING INNOVATION

Protecting consumer privacy in the IoT context is in the early stages of policy review. The paper identifies some of the issues and challenges with privacy, including the need for devices to incorporate privacy-by-design and the use of privacy enhancing technologies. It also points to leveraging existing privacy frameworks, particularly the Federal Trade Commission's privacy framework.[35] Voluntary industry guidelines and codes of conduct predicated on best practices also may be an appropriate means of establishing a framework to protect privacy for new kinds of connected devices. The nature and scope of IoT data flows and their privacy implications are not fully known yet. It is clear, however, that consumers need clear, easy-to-understand privacy policies from device makers.[36]

The green paper calls for, among other things, continuing to convene multistakeholder processes and gather stakeholder feedback on privacy. This approach is the best way to develop a consistent data privacy framework for the entire Internet ecosystem that balances the twin objectives of protecting consumers while promoting innovation in new data-driven services and capabilities.

CONCLUSION

The Internet of Things holds tremendous promise and potential for a host of new products, services and capabilities to enhance every-day life in and outside the home. Cable companies have strong incentives to introduce new IoT devices and support such devices for their residential and business customers and encourage the growth of the IoT by promoting

[35] Green Paper at 31.

[36] BITAG Report at 7.

industry-led IoT standards, and research and development to address IoT security and privacy concerns. Our companies recognize that consumers will not fully embrace the IoT unless they have confidence in the integrity of the data that flows through IoT devices. The green paper is staking out the right course for a public-private partnership to achieve this goal.

Respectfully submitted,

/s/ Rick Chessen

William A. Check, Ph.D.
Senior Vice President, Science & Technology
and Chief Technology Officer

Matt Tooley
Vice President,
Broadband Technology

Rick Chessen
Loretta Polk
NCTA – The Internet & Television Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222- 2445

March 13, 2017