Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Department of Commerce
Washington, D.C.

In the Matter of	)	
	)	
The Benefits, Challenges, and Potential Roles	)	Docket No. 160331306-6306-01
For the Government in Fostering the Advancement	)	RIN 0660-XC024
of the Internet of Things	)	
	)	

Comments of 5G Americas

5G Americas commends the National Telecommunications and Information Administration ("NTIA") for reviewing the current technological and policy landscape impacting the Internet of Things ("IoT") in its request for comment ("RFC").[1] 5G Americas encourages NTIA to focus its upcoming *Green Paper* on supportive and flexible measures that will further IoT advancement.

5G Americas, the leading voice for 5G and LTE in the Americas, is an industry trade organization comprised of our region's national operators and manufacturers. The organization's mission is to foster—throughout the ecosystem in the Americas—the advancement of LTE mobile broadband technology and its evolution beyond into 5G.

5G Americas regularly works with government agencies, regulatory bodies, technical standards organizations, and other global wireless organizations in our efforts to promote seamless interoperability and convergence. This includes 5G Americas' role as a Market Representation Partner in the 3rd Generation Partnership Project ("3GPP"), its membership in

[1] *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, Notice and Request for Public Comment, Docket No. 160331306-6306-01, RIN 0660-XC024, 81 Fed. Reg. 19,956 (Apr. 6, 2016) ("IoT RFC").

the International Telecommunication Union ("ITU") and the Inter-American Telecommunication Commission of the Organization of American States ("CITEL"), and its collaborative working agreements with other agencies throughout the Western hemisphere.

To further its mission, 5G Americas plays a major role in researching and educating the industry on advancements in 3GPP technology. As an example of that leadership, in the last year, 5G Americas has published several IoT and 5G white papers that explore these developments and make industry and government recommendations, including *Cellular Technologies Enabling the Internet of Things*[2] and *5G Technology Evolution Recommendations.*[3] 5G Americas points NTIA to its trove of publicly-available white papers as NTIA navigates this rapidly changing field.[4] While IoT has begun to be deployed in existing cellular and other wireless technologies, 5G, expected to be commercially deployed in 2020, could facilitate IoT through more efficient network management of Massive Machine-Type Communications and other IoT applications.[5]

---

[2] White Paper, *Cellular Technologies Enabling the Internet of Things*, 5G Americas (Nov. 2015), http://www.4gamericas.org/files/6014/4683/4670/4G_Americas_Cellular_Technologies_Enabling_the_IoT_White_Paper_-_November_2015.pdf ("*Cellular IoT* White Paper").

[3] White Paper, *5G Technology Evolution Recommendations*, 5G Americas (Oct. 2015), http://www.4gamericas.org/files/2414/4431/9312/4G_Americas_5G_Technology_Evolution_Recommendations_-_10.5.15_2.pdf ("*5G Evolution* White Paper"); *see also* White Paper, *4G Americas' Recommendations on 5G Requirements and Solutions*, 5G Americas (Oct. 2014), http://www.4gamericas.org/files/2714/1471/2645/4G_Americas_Recommendations_on_5G_Requirements_and_Solutions_10_14_2014-FINALx.pdf ("*Recommendations on 5G* White Paper").

[4] 5G Americas' white papers are available at http://www.4gamericas.org/en/resources/white-papers/.

[5] The appropriateness of "Net Neutrality" rules for IoT should be considered in light of the need for some prioritization of applications. *See, e.g. Could net neutrality stand in the way of traffic safety?* Tech Policy Daily, American Enterprise Institute (June 2, 2016), http://www.techpolicydaily.com/communications/net-neutrality-stand-way-traffic-safety/?utm_source=newsletter&utm_medium=paramount&utm_campaign=cict.

The questions that NTIA raises in its RFC reflect the complex issues accompanying development and implementation of IoT. In response to those questions, 5G Americas comments on (1) identifying characteristics of IoT; (2) requirements for fostering advancement of IoT; (3) domestic and international policy for IoT development; and (4) current work to address IoT security.

I. Internet of Things Characteristics

The NTIA seeks input on the definitions it should "use in examining the IoT landscape."[6] 5G Americas cautions against limiting definitions while technology is constantly changing. At the same time, it is important to understand what IoT can encompass.

5G Americas has previously explained IoT broadly in its *Cellular Technologies Enabling the IoT* White Paper, and encourages NTIA to do the same. The IoT is "a network of physical objects, machines, people and other devices to enable connectivity and communications to exchange data for intelligent applications and services to be developed."[7] IoT, a "natural evolution of Machine-to-Machine (M2M) technology," is the "interconnection of intelligent devices and management platforms that collectively enable the 'smart world' around us."[8] IoT devices include "smartphones, tablets, consumer electronics, connected vehicles, motors and sensors capable of IoT communications."[9] Potential IoT use cases span a diverse range of industries and are virtually unlimited; these include smart irrigation systems,

---

6 IoT RFC at 19,958, Question 2.

7 *Cellular IoT* White Paper at 1, Executive Summary.

8 *Id.* at 4 § 2.1.

9 *Id.* at 1, Executive Summary.

smart buildings, smart meters, smart cities, home energy management, vehicle diagnostics, and more.[10]

Due to the wide range of existing and potential use cases, there are indeed "challenges and opportunities that are novel to IoT," as NTIA recognizes.[11] One of the major challenges is the rate at which IoT applications and devices are increasing. IoT applications "are predicted to grow at a much faster pace than what existing networks and cellular technologies can optimally handle."[12] Recent "market analyses and predictions indicate that the field of IoT is expected to bring a revolution of tremendous growth opportunities with millions of new endpoint and gateway (GW) devices, innovative network infrastructures and new sets of enablement protocols/technologies and exciting applications."[13] Rapid growth requires rapid innovation in network management to meet the demands of technology.

While some of these challenges exist for other technology, IoT applications are also unique in part because of the diversity of technology and the broad range of uses. Smart cars, for example, demand low latency so that there will be no delay in communicating while they are moving in traffic. Some IoT applications on the other hand—such as smart meters or connected streetlamps—will not require regular signals, but will need to operate at low power to extend battery life. Further, the mobility of many of these IoT devices will require the flexibility to move from network to network while maintaining consistent communications.

---

[10] *Id.* at 11 § 3 and 11-12, Table 3.1 (citing oneM2M use cases).

[11] IoT RFC at 19,958, Question 1(b).

[12] *5G Evolution* White Paper at 3 § 2.1.

[13] *Cellular IoT* White Paper at 1, Executive Summary.

II. Fostering Advancement of IoT Technologies

To foster advancement of IoT in light of these challenges and opportunities,[14] NTIA and other agencies must have flexible regimes that support innovation and allow the industry to develop solutions to many of the above-mentioned challenges.[15] Supportive steps for advancing IoT include ensuring availability of sufficient spectrum with flexible use. In turn, such flexible-use policies will encourage infrastructure investment and development.

a. *Spectrum availability will encourage innovation.*

Sufficient spectrum availability is key to IoT development.[16] The IoT will require densification of cellular networks for connected high-speed consumer devices and certain industrial data-intensive applications such as robotics and advanced manufacturing. The IoT will also require networks of industrial narrowband, low-power Machine-Type Communications (MTC) with lower capacity requirements. Even though many industrialized IoT or MTC applications will be much lower-power than consumer broadband devices or access points, new technology for IoT means a surge in mobile wireless data, with increased demands for network management, and the efficient allocation of spectral resources through network slicing and mobility on-demand, and other innovative core and edge technologies.

Diversity of IoT applications requires spectrum in low-, mid-, and high-band ranges of various channel widths. According to Julius Knapp, Chief of the Federal Communications

---

[14] *See* IoT RFC at 19,957 ("NTIA is requesting comment on the benefits, challenges, and potential roles for the government in fostering the advancement of the [IoT]").

[15] *See, e.g., id.* at 19,959, Question 6 (seeking input on technological issues that could hinder the development of IoT); *see also id.*, Question 10 (asking about government role in "bolstering and protecting the availability and resiliency of these infrastructures to support IoT").

[16] *See id.* at 19,959, Question 6(a)(iii) (asking whether spectrum availability may be a possible technological issue for development of IoT).

Commission's Office of Engineering and Technology, the Commission's decisions are moving away from "service-specific spectrum" so that "the Commission's flexible rules in both unlicensed and licensed bands" can "obviate the need for allocations narrowly tailored to specific uses."[17] Knapp provides the rationale for flexible rules: they allow business to "focus on locating spectrum that best matches their need, with higher-frequencies best accommodating high-bandwidth applications, and lower bandwidths accommodating uses requiring wider area coverage."[18]

In short, higher, mid, and lower bands are important for IoT development.[19] For instance, low-band spectrum is crucial for both consumer broadband devices and for Massive MTC where coverage is a critical factor (e.g., seismic sensors). And wide channelized millimeter wave spectrum would be ideal for applications that require very low latency in smaller areas with very high throughput, like industrial IoT smart manufacturing. Self-driving connected cars will require both low latency and high-throughput, so will require both low- and high-band spectrum. To best accommodate the variety of applications within IoT, the industry needs a broad range of additional spectrum for continued development. Additional spectrum—with flexible use rules—is vital for the United States to retain its leadership in innovative

---

[17] Julius Knapp, Chief, Office of Engineering and Technology, Federal Communications Commission, Comments at the 2014 Winnik Forum (Nov. 2014).

[18] *Id.*

[19] *See 5G Evolution* White Paper at 8 § 3.1, 22 § 4.2.9, and 30 § 6.2.

wireless applications. 5G Americas encourages NTIA to continue identifying spectrum bands to repurpose for commercial use, consistent with the President's directive.[20]

b. IoT will require updates to network infrastructure.

IoT will also place unique demands on infrastructure.[21] Infrastructure must evolve along with the creation of IoT technology to support the increasing demands of the billions of connected devices projected to enter the market. Network infrastructure will not only need to be "highly scalable in terms of its capacity" but also able to "optimally handle differing service needs of various IoT verticals."[22] IoT service requirements include the need for "mobility, latency, network reliability and resiliency."[23] Meeting these requirements will entail "re-architecting key components of the cellular network, such as to support mobility on-demand only for those devices and services that need it."[24]

5G Americas has explored functional architecture and commonly-used protocols in IoT. A typical end-to-end architecture for IoT solutions includes the device or gateway, access network, mobile core network, connectivity platform, and application platform. These components are currently being optimized for IoT or Massive MTC applications. For instance, there has been a push to optimize the 3GPP core network for IoT services and devices,

---

[20] *See* Presidential Memorandum, *Expanding America's Leadership in Wireless Innovation*, The White House (June 14, 2013), https://www.whitehouse.gov/the-press-office/2013/06/14/presidentialmemorandum-expanding-americas-leadership-wireless-innovatio.

[21] *See* IoT RFC at 19,959, Question 8 ("How will IoT place demands on existing infrastructure architectures, business models, or stability?").

[22] *5G Evolution* White Paper at 3 § 2.1.

[23] *Id.*

[24] *Id.*

including ongoing MTC work in 3GPP and the application of Network Functions Virtualization (NFV) and Software-Defined Networking (SDN) technologies to support use cases more efficiently.[25] While NFV and SDN were originally developed for enhanced mobile broadband, their more efficient functionality will help facilitate IoT as well.

IoT also requires other network-related solutions, including alternative access method enablement; the provision of seamless connectivity via multiple access technologies; remote and automated operation, administration, management and provision; virtualization on the majority of network domains; and discoverability of data, services and applications via search engines.[26] As IoT applications continue to expand, network architecture must continue to evolve. Accordingly, businesses will seek to adjust their models to leverage these applications for their customers' benefit. 5G Americas provides communication service providers with guidelines for IoT business models and solutions for forming effective IoT strategies.[27] Steps include updating business models, identifying the technology implications, securing IoT services and information assets, and updating management platforms.[28] As businesses face these challenges, they will need a supportive environment from agencies and regulators to allow for ease of implementing IoT.

---

[25] *Cellular IoT* White Paper at 22-24 § 4.1.

[26] *Cellular IoT* White Paper at 22-24 § 4.1 and 57, Appendix A.

[27] *Id.* at 57, Appendix A.

[28] *Id.* at 57-59, Appendix A.

III. Domestic and International Policy

The RFC seeks input on "how to best monitor and/or engage in various international fora" to encourage innovation and growth of the digital economy.[29] Specifically, NTIA wants input on factors it should consider in its international engagement in standards and specification organizations, industry alliances, and other bodies.[30] With respect to the International Telecommunication Union, an inter-governmental body of the United Nations, the United States should support policies that promote international harmonization of spectrum at the broad service level, and not harmonization of spectrum for specific IoT applications themselves. Rather, the decision to apply particular IoT applications in particular spectrum bands should be left to industry. IoT will develop best if allowed to be deployed under flexible-use policies. With respect to technical standards bodies, while it is important for the United States to be aware of the work within international standards bodies, any role of NTIA should be that of supporting industry efforts at standardization. NTIA should oppose efforts of other governments or inter-governmental bodies to develop technology standards for IoT, which would only limit its innovation.

As a general matter, regional and global harmonization of spectrum bands at the service—not application—level is beneficial to consumers because it provides the U.S. ecosystem with economies of scale, reduces overall cost to consumers, and provides "faster adoption and proliferation of the technology."[31] A 5G application like IoT can benefit from

---

[29] IoT RFC at 19,959, Question 19.

[30] *See id.* at 19,959, Question 20.

[31] *Comments of 5G Americas* at 14, GN Docket No. 14-177, et al. (filed Jan. 27, 2016); *5G Evolution* White Paper at 49 § 8.

harmonization of bands considered by international and regional organizations, but 5G Americas cautions against identification of specific bands for IoT. At its World Radiocommunication Conference held in 2015 (WRC-15), the ITU Radiocommunication Sector (ITU-R) was invited to study for possible identification spectrum needed for Machine-to-Machine communications and study possibly harmonizing bands for MTC for the next conference, WRC-19.[32] 5G Americas represents NTIA not to support such an application-specific approach for IoT with the ITU, particularly given that the technical characteristics of IMT 2020 are being developed by ITU-R working parties, including for IMT 2020 applications like MTC for purposes of spectrum sharing studies.

On the domestic side, the FCC plans to issue flexible-use licenses in millimeter wave spectrum, as it has before in low- and mid-band spectrum for 3G and 4G.[33] Flexible-use licenses will allow licensees to continue to innovate. The FCC will not require particular technologies or applications—IoT or otherwise—to be deployed. This is a useful model for spectrum assignment because it allows permissionless innovation. While spectrum-sharing systems (e.g., TV White Space, Dynamic Spectrum Access, and Spectrum Access System databases) that the FCC is exploring have promise, they remain in their infancy as a means to ensure IoT is spectrum agnostic. Technology-neutral policies and flexible use are critical for IoT development, and NTIA should support this flexibility as it works with the FCC on mitigation techniques to share spectrum between federal systems and commercial use.

---

[32] *See* World Radiocommunication Conference, Resolution 958, Agenda Item 9.1.8 (WRC-15).

[33] *Use of Spectrum Bands Above 24 GHz For Mobile Radio Services*, GN Docket No. 14-177, Notice of Proposed Rulemaking, FCC 15-138, 30 FCC Rcd. 11,878 (rel. Oct. 23, 2015).

OET Chief Julius Knapp has said that because of the diversity of technology within IoT, dedicating spectrum for narrow types of smart devices, tracking utilities, and machine-to-machine communications would waste limited resources.[34] 5G Americas agrees that flexibility for spectrum use is ideal, and specific bands should not be identified for specific IoT applications. As for designation of spectrum for 5G generally, which can encompass both Massive MTC, enhanced mobile broadband, and low-latency, ultra-reliable applications like connected cars and remote surgery, the United States should continue exploring and encouraging bands that were proposed by CITEL for WRC-15 and designated for study for WRC-19.[35]

Many significant developments for IoT are taking place in international industry alliances, standards bodies, and specifications organizations, as the RFC acknowledges.[36] These groups allow industry stakeholders and experts to participate in crafting policies and requirements for the continuous development of IoT. Because the private sector is in the best position for setting standards that encourage innovation, the ITU Telecommunication Standardization Sector ("ITU-T"), an inter-governmental body, should not be encouraged by the U.S. government to assume a leading role in ITU-T standardization, for example, through Study Group 20 IoT. While information gathering and study is important, the private sector should take the leading role in setting standards, not an inter-governmental body. Likewise, the European Commission apparently contemplates a government role in directing its industry to

---

[34] Julius Knapp, Comments at the 2014 Winnik Forum.

[35] *See Recommendations on 5G* White Paper at 8-9 § 3.1.3; 12 § 5.1; 18 § 7.

[36] IoT RFC at 19,959, Questions 20(a) and (c).

focus on IoT standards, as one of the key technologies undergirding its plans for the Digital Single Market.[37] While 5G Americas applauds the European Commission's focus on IoT and encourages dialogue between policymakers on both sides of the Atlantic, it does not support any formal arrangement for governments to collaborate on the development of technical standards for IoT or 5G technology. U.S. government monitoring of activities within the private sector standards bodies and other international organizations is certainly encouraged to keep the policymakers and the agencies up to date.

IV. Security for the Internet of Things

The RFC asks about cybersecurity concerns raised specifically by IoT and how those concerns change based on categorization of IoT.[38] Security is a high priority for the wireless industry generally and 5G Americas members specifically.[39] Security has been developed and deployed for cellular technology since 2G and has been enhanced in 3G and 4G technology evolutions, as a market imperative. As technology transitions to the next generation, working groups are actively collaborating to evolve existing security measures that have already been developed to adapt to networks with billions of devices and IoT endpoints. Many low-power industrial IoT nodes will be deployed in unlicensed spectrum. IoT deployed over cellular

---

[37] *See* Press Release, *Commission sets out path to digitise European industry*, European Commission (Apr. 19, 2016), http://ec.europa.eu/growth/tools-databases/newsroom/cf/itemdetail.cfm?item_id=8785.

[38] IoT RFC at 19,959, Question 16.

[39] GSMA, another mobile industry association with some membership overlap, but with global as opposed to regional reach like 5G Americas, has recently held a conference dedicated to 5G and IoT security and privacy. *See, e.g.* GSMA Mobile 360 Series – Privacy and Security, The Hague, Netherlands, May 10-11, 2016, http://www.gsma.com/gsmaeurope/event/mobile-360-series-privacy-and-security/.

technologies in licensed spectrum can benefit from the enhanced security a managed network can bring. The best way for security measures to address the diverse range of IoT applications is for the relevant industries to apply their knowledge in working groups and industry organizations to create effective security measures consistent with existing legal standards.[40] 5G Americas members are engaged in various standards bodies and industry coalitions addressing 5G security, many of which focus on specific IoT use cases for security. Industry stakeholders are incentivized to ensure their systems are secure, and they are in the best position to develop the technology to address their customers' ever-changing threats.[41] Government agencies should avoid imposing security measures that may rapidly become obsolete or ineffective as technologies continue to evolve.

3GPP has developed specific working groups to address security issues for 5G, including next-generation mobile broadband systems and IoT technology. One of these groups is the 3GPP SA3 Working Group, which is investigating security needs for V2X communication (encompassing vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-pedestrian communication) and next-generation mobile broadband systems. The group's efforts include identifying security threats, defining security requirements, and proposing potential solutions in a series of technical reports. Recently, 3GPP SA3 initiated a study item for

---

[40] The Federal Trade Commission has taken a number of enforcement actions to ensure that IoT products provide the security marketed by their vendor. *See, e.g.*, Press Release, *Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy*, Federal Trade Commission (Sept. 4, 2013), www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-homes. *See also* FTC Staff Report, *Internet of Things: Privacy and Security in a Connected World* (January 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[41] *See* Letter from Patricia Paoletta, Partner, Harris, Wiltshire & Grannis LLP to Marlene H. Dortch, Secretary, Federal Communications Commission, GN Docket No. 14-177, et al. (Apr. 8, 2016) (discussing 5G security).

Security Aspects for LTE support of V2X services based on the use cases and potential requirements for LTE support for vehicular communications services and potential architecture enhancement. Part of this process includes reviewing input from stakeholder companies and making specialized recommendations based on their input.

Other industry standards groups are working on safety and security for IoT in parallel. The wireless industry and the vertical industry of automotives are coordinating through existing automotive industry standards groups such as Society of Automotive Engineers (SAE) and the International Electrotechnical Commission (IEC). These groups are working on cybersecurity and other safety aspects for connected cars.

Industry-specific standards development organizations are best situated to address cybersecurity and safety concerns and have the flexibility to create new specialized working groups and studies as new technology develops. Accordingly, 5G Americas encourages agencies like NTIA to follow those activities for informational purposes so as to be assured of these organizations' specialized knowledge in creating security measures.

V. Conclusion

Any government policies must support technology evolution so the United States can remain a forum for IoT innovation and U.S. citizens can benefit from enhanced productivity and other societal goods that flow from IoT applications. The United States should continue to support IoT consistent with technology neutrality and flexible spectrum use, in both licensed and unlicensed spectrum. In other words, there is no need to allocate specific bands of spectrum for specific IoT applications. Similarly, the U.S. government should not mandate security measures while these standards are actively being developed, particularly since the success of security in IoT is a market imperative. The United States should continue to support policies

that promote international harmonization of services (e.g., mobile or fixed services, etc.) that will provide the spectrum for these innovative applications to be deployed under flexible-use policies. Making sufficient spectrum available, allowing flexibility for development, and encouraging other governments to support industry-driven standardization will facilitate U.S. technology leadership on IoT, as well as benefit American citizens with innovative applications to enhance their social and professional lives.

Respectfully submitted,

Chris Pearson

President, 5G Americas
1750 Avenue, N.E., B220
Bellevue, WA 98004
O: 425 372 8922
www.5gamericas.org

June 2, 2016