Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of	)	
	)	
The Benefits, Challenges, and Potential Roles for the	)	Docket No. 1603311306-6306-01
Government in Fostering the Advancement of the	)	RIN 0660-XC024
Internet of Things	)	
	)	

COMMENTS OF THE CONSUMER TECHNOLOGY ASSOCIATION F/K/A THE CONSUMER ELECTRONICS ASSOCIATION

CONSUMER TECHNOLOGY ASSOCIATION F/K/A CONSUMER ELECTRONICS ASSOCIATION

Julie M. Kearney
Vice President, Regulatory Affairs
Alexander B. Reynolds
Director, Regulatory Affairs
Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7644

June 2, 2016

Table of Contents

Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 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. 1603311306-6306-01 RIN 0660-XC024
	)	

THE CONSUMER TECHNOLOGY ASSOCIATION F/K/A THE CONSUMER ELECTRONICS ASSOCIATION

I. INTRODUCTION

The Consumer Technology Association ("CTA")[1] applauds the Department of Commerce ("Department") for its continued effort to promote the Internet of Things ("IoT"), and, in particular, for issuing the above-captioned Request for Comment ("RFC")[2] soliciting input on how to develop a more cohesive federal government approach that will foster IoT innovation and economic growth.[3] CTA is proud to represent the companies whose products and

[1] The Consumer Technology Association ("CTA")™, formerly the Consumer Electronics Association ("CEA")®, is the trade association representing the $285 billion U.S. consumer technology industry. More than 2,200 companies – 80 percent are small businesses and startups; others are among the world's best known brands – enjoy the benefits of CTA membership including policy advocacy, market research, technical education, industry promotion, standards development, and the fostering of business and strategic relationships. CTA also owns and produces CES® – the world's gathering place for all who thrive on the business of consumer technology. Profits from CES are reinvested into CTA's industry services.

[2] *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, Request for Public Comment, Docket No. 1603311306-6306-01, RIN 0660-XC024, 81 Fed. Reg. 19,956 (Apr. 6, 2016) ("RFC").

[3] *See* Davidson and Kinney, *supra*; *see also* Lawrence E. Strickling, Assistant Sec'y of Commerce for Commc'n and Info., Dep't of Commerce, Keynote Address at the Silicon Flatirons Conference on the Digital Broadband Migration: The Evolving Industry Structure of the Digital Broadband Landscape (Jan. 31, 2016) (indicating that the National Telecommunications and Information Administration, an agency within the Commerce Department, would issue a request for comment regarding whether there are policy areas related to the IoT that could be appropriate for multistakeholder engagement), http://1.usa.gov/1sOUaVa.

services largely comprise the IoT and looks forward to working with the Department and other stakeholders on this initiative.

The RFC aptly recognizes that the IoT "has quickly become one of the most important technological trends of this decade. It touches almost every industry and will transform our lives and society worldwide."[4] Indeed, whether you call it the "Internet of Things," the "Internet of Everything," the "Connected World," or just plain amazing, the rapidly expanding thread of connectivity among everyday objects via the Internet unquestionably is changing how the world works. Thermostats, refrigerators, and even whole factories of equipment can harness the power of the Internet to provide enormous personal, economic, and societal benefits—some we already see, and some are yet to be imagined. Today, consumer- and industrial-facing IoT applications save consumers and businesses time and expense, increase efficiency and productivity, promote public health and safety, and serve as key economic drivers that enhance the U.S. role as a global leader in technology.[5]

Nowhere are the opportunities and promise of the IoT more evident than at the annual CES in Las Vegas, which is the most popular technology trade show in the world and arguably the most important annual innovation event worldwide. From around the globe, thousands of companies display an awe-inspiring vision of the future and showcase the latest and greatest IoT technologies. Walking the show floor in 2016, visitors saw a vision of the connected world that was jaw-dropping in its expanse and potential: multitudes of devices communicating with each other to improve quality of life across many metrics, with enormous potential to beneficially transform our lives and society. Its seamless connectivity, made possible by increased

[4] Press Release, Dep't of Commerce, *U.S. Department of Commerce Seeks Comment on Potential Policy Issues Related to Internet of Things*, Apr. 5, 2016, http://1.usa.gov/1ozo253 ("Comment Press Release").

[5] *Id.* ("The explosive growth of connected devices promises both enormous benefits and complex challenges in areas such as health, safety, energy, security, and the environment.").

processing power and tiny sensors, will enable machines and devices to respond to conditions and situations pursuant to parameters dictated by a consumer—for example, running the washing machine at a time of day when energy costs are low. The IoT connected world will improve energy conservation, efficiency, productivity, public safety, health, education, and more. It will enable more smart homes and appliances, smart cars, smart retail experiences, smart agriculture and manufacturing, and smart devices we cannot imagine today. These connected devices and machines will make our lives easier, safer, healthier, less expensive, and more productive.

This is just the beginning, and there is no telling what the future holds. As Assistant Secretary Strickling explains, "We are just beginning to see the exciting range of novel applications and connected devices emerging from the Internet of Things."[6] Explosive gains in IoT connectivity and the lightning-fast speed of innovation in general are driving strong growth across countless tech categories, as well as sparking growth with new capabilities and new business models across multiple industry sectors. As highly sophisticated technology becomes more affordable and accessible, new innovations will help improve our safety, productivity, and entertainment. And the next evolution of the IoT will build on connections already in place. As products become smart and connected, consumers will be able to manage their lives and engage in work in ways that were not even imaginable a decade ago.

The Department's green paper to be produced based on input responding to the RFC should recognize that policymakers must work *with* industry to ensure that any actions taken in the name of consumer protection do not inadvertently hamstring the myriad consumer-friendly IoT developments. Government must allow consumers and the market to decide IoT winners and losers, rather than dictating outcomes itself. Policymakers thus should focus on private

[6] *Id.*

sector, consensus-driven industry self-regulation, which has a proven history of minimizing consumer harms while maximizing flexibility to innovate, instead of government action that threatens to curb innovation.

In addition, policymakers should encourage and support growth and adoption of the IoT through efforts to spur research and development, lower effective tax rates, adopting immigration policies that allow U.S. companies to attract the best and brightest, and aggressively facilitating access to spectrum. The government can best promote consumer confidence and trust in the IoT under applicable *existing* statutes and regulations; these existing legislative and regulatory vehicles will ensure protection of consumer privacy, sensitive data, and network security.

II. RESPONSES TO RFC QUESTIONS

A. Challenges and Opportunities Arising from IoT (Question 1)[7]

A significant challenge presented by the IoT is the current fragmented approach of federal government agencies toward its development. The RFC notes that a number of federal agencies—for example, the National Highway Traffic Safety Administration ("NHTSA") and the Food and Drug Administration ("FDA")—have already begun grappling with potential health, safety, and security issues arising from the connection of cars and medical devices to the Internet, while the Federal Trade Commission ("FTC") has identified consumer privacy and cybersecurity aspects of IoT and proposed some possible best practices, and the Administration is sponsoring grants for Smart Cites through no less than five agencies. Many of these efforts are critical to the long-term success of the IoT, but the fragmentation is potentially damaging.[8]

[7] Section I, above, also discusses the opportunities and benefits of the IoT.

[8] *See* Darren Samuelsohn, *What Washington really knows about the Internet of Things*, Politico ("new networked-object technologies are covered by at least two dozen separate federal agencies—from the [FDA] to the National Highway Traffic Safety Administration ("NHTSA"), from aviation to agriculture—and more than 30 different congressional committees"), http://politi.co/1Kk0usb.

This fragmentation and duplication of effort reflects the fact that, as the RFC notes, "some types of devices will fall into readily identifiable commercial or public sectors in their own right—for example, implantable health devices—but most will serve the function of enabling existing industries to better track, manage, and automate their core functions."[9] The FDA's rules and the Health Insurance Portability and Accountability Act ("HIPAA," enforced by the Department of Health and Human Services) may apply to a wearable offered by your health provider, whereas the same device, purchased in a retail store, may be regulated in an entirely different manner, such as by the FTC. Meanwhile, the federal agency that has been the most involved in exploring the consumer IoT, the FTC, is focused on a case-by-case law enforcement approach and providing broader guidance by interfacing with IoT companies by convening workshops and issuing business guidance but ultimately its legal authority has some limitations.[10] Thus, the specific laws, rules, and regulatory regime(s) that apply to a particular IoT device or application may not always be obvious and may even overlap or conflict, and this complex web may be particularly difficult for smaller companies unable to afford counsel for each regime to navigate.

These challenges are exacerbated as innovation eviscerates historical distinctions between different types of services and applications. As the Department's Alan Davidson and Linda Kinney recently described,

> Regulators have long been focused on health and safety regulations that protect consumers; but in the past, enterprises in the transportation,

[9] RFC at 19,957.

[10] On the other hand, the FTC's general Section 5 authority covers broad swaths of industries, and thus it is not constrained on a sector-specific basis in the same way as is, for example, the Federal Communications Commission ("FCC"). The FTC can set parameters through enforcement actions based on specific entities' business practices that are deceptive or unfair to consumers (*e.g.*, failing to adequately protect consumer data or not meeting the terms of a privacy policy or other representations to the consumer).

> healthcare, and communications sectors have mostly functioned and been regulated independently. Now our physical and digital worlds are converging and lines between industries are increasingly blurred. Automobiles are becoming communications devices on wheels…. [T]he Internet of Things is breaking down traditional silos….[11]

Moreover, legislative and regulatory vehicles that would focus on IoT-specific technologies, rather than IoT as part of larger and more comprehensive legislation, or inappropriate use of a given IoT application, are a mistake. They would threaten to put the government in the position of picking winners and losers to the detriment of competition, innovation, economic growth, and, ultimately, consumer and societal welfare. Instead, policymakers should focus on desired outcomes and results, and let the pace of innovation and market dynamics determine which IoT technologies prevail. The Department's own staffing structure recognizes this challenge, which it describes as "the cross-cutting nature of the IoT landscape."[12]

Of course, there are other challenges to the success of the IoT beyond inconsistent, premature, and reactionary regulatory regimes. At a fundamental level, the IoT depends in great part on the collection and sharing of information among devices and machines, and thus is premised on consumer trust, data accuracy, and utility. IoT manufacturers and service providers take seriously the need for consumer trust and, both as individual companies and as industries, have proactively addressed these issues. Moreover, the current lack of IoT technical standards muddies the water for players in the IoT ecosystem, who have no agreed-upon regimen for how

[11] Alan Davidson and Linda Kinney, *Fostering Investment and Innovation in Smart Cities and the Internet of Things (IoT)*, NTIA (Feb. 25, 2016, 3:52 PM) (this "growing global patch of regulation threatens to increase costs and delay the launch of new products and services", which "in turn, could dampen investment"), http://1.usa.gov/1Q5i5Xd.

[12] RFC at 19,958.

to connect or interoperate. As discussed below, the Department can take several steps to encourage and support the IoT.

B. Definition to Use in Examining the IoT Landscape (Question 2); Ways to Divide or Classify the IoT Landscape to Improve the Precision with which Public Policy Issues are Discussed; Benefits or Limitations of Using Such Classifications (Question 4)

CTA recommends that the Department consider consumer-facing applications (the "Consumer IoT"), as distinct from industrial, commercial, and enterprise applications. Consumer applications represent less than one-third of the IoT's potential economic value.[13] It is especially critical for policymakers to understand this distinction and ensure both categories of IoT development—consumer and industrial/commercial/enterprise—are not curbed by over-regulation. Further, policymakers must recognize that consumer data can provide broader public interest benefits, *e.g.*, using data from smart thermostats for grid management and traffic data from mobile phones for smart city development. In this vein, CTA applauds the recent creation of the bipartisan, congressional Internet of Things Working Group, which aims to educate Members and bring them "up to speed on this technology and its impact on the modern economy and consumers."[14]

[13] *See* James Manyika *et al.*, *Unlocking the potential of the Internet of Things*, McKinsey Global Institute (June 2015) ("Business-to-business applications will probably capture more value—nearly 70 percent of it—than consumer uses….") ("*Unlocking the Potential*"), http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

[14] Rep. Bob Latta (R-OH) and Rep. Peter Welch (D-VT), *The Internet of Things has the potential to be the engine that powers our economy for decades to come*, The Hill Congress Blog (May 31, 2016 9:01 AM), http://thehill.com/blogs/congress-blog/technology/281495-the-internet-of-things-has-the-potential-to-be-the-engine-that.

C. Current or Planned Laws, Regulations, and/or Policies that Apply to IoT (Question 3)

As observed in the RFC, the Department's "long standing technological and policy expertise" can help foster the IoT and its related economic benefits.[15] In addition, the Department's U.S. Patent and Trademark Office ("USPTO") can continue its efforts to improve "patent quality, especially in new technological domains, including IoT."[16] As more "things" become embedded with patentable technologies, the "attack surface" for patent assertion entities—better known as "patent trolls"—grows. Patent reform, enabled by Congress and implemented by the USPTO, aimed at blunting patent trolls will remove a harmful tax on IoT development. And, as discussed in more detail below, spectrum policy, privacy and cybersecurity, and international standards have the potential to encourage or hinder the IoT, making it important that the U.S. does this right.[17]

D. Technological Issues That May Hinder IoT Development (Question 6)

Interoperability and voluntary global standards. A certain level of standardization and interoperability is necessary to achieve a successful, IoT ecosystem. In the emerging IoT economy, voluntary global standards accelerate adoption, drive competition, and enable cost-effective introduction of new technologies. Open standards which facilitate interoperability across the IoT ecosystem will stimulate industry innovation and provide a clearer technology

[15] RFC at 19,958; *see also id.* (noting the that the "Department's National Institute of Standards and Technology (NIST) has coordinated the development of a draft reference architecture for Cyber-Physical Systems and is conducting a Global City Teams Challenge to foster the development of Smart Cities and promote interoperability, NTIA's spectrum planning and management activities contemplate the growth of IoT, and its Institute for Telecommunications Sciences (ITS) has begun testing the possible effects of IoT on spectrum usage"); *id.* ("The mission of the Department is to help establish conditions that will enable the private sector to grow the economy, innovate, and create jobs.").

[16] RFC at 19,958.

[17] *See* Sections II.I and II.J, *infra*, discussing several current initiatives that apply to IoT. Similarly, as noted in Section II.F, the recently enacted FAST Act can encourage the development and development of transportation-related IoT applications.

evolution path. To the extent that interoperability and reliability are related, enabling manufacturers and consumers to create a feedback loop will better calibrate end-user expectations and lead to more useful, cheaper IoT applications, than any government mandate.

Industry is in the best position to develop the technological standards and solutions to address global IoT ecosystem opportunities and challenges. Government should encourage industry to collaborate in open participation global standardization efforts like the Industry Internet Consortium and Open Connectivity Foundation to develop technological best practices and standards.[18] Specifically, government should encourage—not but mandate—the use of commercially available solutions to accelerate innovation and adoption of IoT deployments. Nor should the government mandate security standards. Consumer trust is critical for the IoT to succeed, and companies thus have a built-in incentive to protect data collected and used by IoT devices. The emphasis on commercially available solutions and market-adopted voluntary standards will allow for faster adoption and increase innovation, bringing the IoT and its benefits to reality sooner.

Spectrum availability and potential congestion/interference. Improved access to spectrum is critical to fueling the IoT. To connect the 50 billion devices that will be in use by 2020, a network would require capacity that is "at least 1,000 times the capability that exists today."[19] With the IoT showing promise in so many sectors of our economy, a broad range of

[18] *See* About Us, Industry Internet Consortium, ("The Industrial Internet Consortium was founded in March 2014 to bring together the organizations and technologies necessary to accelerate the growth of the Industrial Internet by identifying, assembling and promoting best practices. Membership includes small and large technology innovators, vertical market leaders, researchers, universities and government organizations."), http://www.iiconsortium.org; OCF-About, Open Connectivity Foundation ("The Open Connectivity Foundation (OCF) is creating a specification and sponsoring an open source project to make this possible.... OCF will help ensure secure interoperability for consumers, business, and industry."), http://openconnectivity.org.

[19] Murray Slovick, *5G: The Mobile Tech of 2020*, CTA i^3, 20 (Nov./Dec. 2014), http://cdn.coverstand.com/25838/232265/711ba5485b2b1c66036f89c895b2-baecbaa98e91.23.pdf.

agencies must partner among themselves and with industry to ensure sufficient spectrum to match the needs of the IoT. The wide variety of IoT spectrum uses means that the Department's National Telecommunications and Information Administration ("NTIA") must help facilitate sharing and/or clearing of federally-controlled spectrum. Given the cross-cutting nature of IoT, agencies must collaborate to enable the IoT to flourish. The joint letter signed by the leaders of the FCC, Department of Transportation ("DOT"), and the Department committing to a testing plan for shared uses in the 5.9 GHz band, is an interagency collaboration that could help, should the agencies follow through on this commitment.[20] If successful, it could be replicated elsewhere, as well as demonstrate a commitment to the consultation advice of industry.

Recognizing that the federal government is the largest single holder of spectrum in the country, federal agencies must share, and where possible clear, spectrum "to ensure the IoT industry has access to the spectrum it needs to continue to grow and change our lives for the better."[21] Public statements recognizing the importance of spectrum and the IoT are starting to

[20] Letter from Penny Pritzker, Sec'y, Dep't of Commerce, Anthony Foxx, Sec'y, Dep't of Transp., and Tom Wheeler, Chairman, Fed. Commc'ns Comm'n, to John Thune, Chairman, Senate Committee on Commerce, Sci., and Transp. (Jan. 2016), http://src.bna.com/bZt.

[21] Press Release, CTA, *Future IoT Success Depends on Access to Spectrum, CTA Says* (Mar. 3, 2016) , http://www.cta.tech/News/News-Releases/Press-Releases/2016-Press-Releases/Future-IoT-Success-Depends-on-Access-to-Spectrum,.aspx (quoting CTA President and CEO Gary Shapiro in support of the Developing Innovation and Growing the Internet of Things Act).

build support for agency action.[22] Even some of the bills currently pending before Congress have the potential to increase available spectrum for commercial uses, including the IoT.[23]

NTIA should also keep in mind the wide range of use cases, and fitting for such a wide range, adopt a technologically neutral approach to the IoT policy framework. The incredible variety of applications in consumer, industrial, commercial, and enterprise spaces means that different kinds of spectrum will be suitable in different situations, including those delivered by wireline, wireless, and satellite. Lower frequencies will be important for coverage and distance in some applications; higher frequencies will also have their value and applicability for IoT. By not favoring any single technology, NTIA can encourage the growth of IoT services across platforms, which will ensure that the best technology is available for each existing and future use case.

E. Factors the Department and Government More Generally Should Consider When Prioritizing Technical Activities with Regard to IoT (Question 7)

The NTIA and the National Institute of Standards and Technology ("NIST") must continue important research into how spectrum can be shared and measured.[24] NIST's cybersecurity framework—the research underlying the framework and the private-public

[22] *See, e.g.*, Cory Booker, Kelly Ayotte, Brian Schatz, and Deb Fischer, *Policymakers Must Look Ahead to Realize the Potential of the Internet of Things*, CTA i^3 (Mar. 10, 2016), http://www.cta.tech/i3/Move/2016/March-April/Policymakers-Must-Look-Ahead-to-Realize-the-Potent.aspx; Bob Latta and Michael O'Rielly, *Improving the 5.9 GHz Band to Enhance Unlicensed and Wi-Fi Networks*, The Hill: Congress Blog (Mar. 2, 2016, 9:00 AM), http://thehill.com/blogs/congress-blog/technology/271408-improving-the-59-ghz-band-to-enhance-unlicensed-and-wi-fi.

[23] *See, e.g.*, Developing Innovation and Growing the Internet of Things Act, S. 2607, 114th Cong. (2016); MOBILE NOW Act, S. 2555, 114th Cong. (2016); Wi-Fi Innovation Act, H.R. 821 and S. 424, 114th Cong. (2016).

[24] In particular, NTIA has been responsive to the recommendations of the Commerce Spectrum Management Advisory Committee ("CSMAC") with respect to industry-government collaboration and spectrum sharing. Paige R. Atkins, Assoc. Adm'r, Nat'l Telecomm. and Info. Admin., *CSMAC Recommendations: NTIA Preliminary Response* (Dec. 2, 2015) (observing that many of CSMAC's recommended actions are already initiated or are a part of on-going NTIA activities), http://1.usa.gov/20yhS2j.

collaboration as the framework developed—is an example of a beneficial technical activity that should be replicated with respect to IoT. As discussed above, given that the numerous IoT technologies will vary depending on IoT use case—from Bluetooth to Wi-Fi to Cellular to Ethernet—it would not make sense to allocate "IoT spectrum." The best enabler is to generally and flexibly open up new licensed and unlicensed spectrum to accommodate any and all communications technologies that may be needed for foreseeable and non-foreseeable IoT use cases.

F. Role of Government in Bolstering and Protecting Availability and Resiliency of Infrastructures to Support IoT (Question 10)

The Department correctly observed that "infrastructure investment, innovation, and resiliency (such as across the information technology, communications, and energy sectors) will provide a foundation for the rapid growth of IoT services."[25] CTA's members are investing heavily in next generation cellular (5G) and next generation Wi-Fi technologies and look forward to partnering with the public sector as part of the Administration's Smart Cities Initiative, which will "invest over $160 million in federal research" to leverage IoT "to improve the life of … residents."[26] Similarly, CTA is closely following DOT action in response to the recently enacted FAST Act.[27] The FAST Act rightfully permits the DOT greater flexibility with respect to various surface transportation funding allocations and programs to be used on

[25] RFC at 19,959.

[26] Press Release, The White House, *FACT SHEET: Administration Announces New "Smart Cities" Initiative to Help Communities Tackle Local Challenges and Improve City Services* (Sept. 14, 2015), http://1.usa.gov/1MttsZD. The new capabilities and services made possible by the IoT require advancement and investment in our current infrastructures in order to securely deliver, grow, and scale adoption. Our current networks do not have the capacity to transmit, secure, or store the explosion of data that is being generated by the fifty billion estimated devices connecting by 2020.

[27] Fixing America's Surface Transportation Act, Pub. L. No. 114-94, 129 STAT. 1312, (2015).

technology deployment, including Intelligent Transportation System technologies and other applications of the IoT.[28]

The government has played a critical role in building infrastructure in other contexts. For example, to promote broadband deployment as a high priority, President Obama issued Executive Order ("E.O.") No. 13616, "Accelerating Broadband Infrastructure Deployment,"[29] to facilitate wired and wireless broadband infrastructure deployment in federal lands and buildings. Among other things, the E.O. established a working group comprised of representatives from fourteen federal agencies and offices, whose task was to ensure a coordinated approach in implementing agency procedures, requirements, and policy with respect to broadband deployment on federal lands and buildings. In one short year, the working group made a number of process and policy improvements designed to promote broadband deployment, including coordinating consistent and efficient federal broadband procedures, coordinating use of uniform contracts and applications, and establishing best practices for excavations for the installation of broadband facilities during federal or federally assisted highway construction.[30]

Likewise, President Obama on March 23, 2015 signed a Presidential Memorandum[31] creating the Broadband Opportunity Council ("Council"), co-chaired by the departments of Commerce and Agriculture and comprised of twenty-five federal agencies and departments, to "engage with industry and other stakeholders to understand ways the Executive Branch can

[28] CTA also eagerly anticipates the DOT report on the "Potential of the Internet of Things," which Congress directed the DOT to create by June 4, 2016. *Id.* § 3024, 129 Stat. at 1494.

[29] Exec. Order No. 13616, 77 Fed. Reg. 36903 (June 20, 2012), http://1.usa.gov/1SNR1vy.

[30] Broadband Deployment on Federal Property Working Group, *Implementing Executive Order 13616: Progress on Accelerating Broadband Infrastructure Deployment*, Progress Report to the Steering Committee on Federal Infrastructure Permitting and Review Process Improvement (Aug. 2013), http://1.usa.gov/1O5MyqP.

[31] Memorandum on Expanding Broadband Deployment and Adoption by Addressing Regulatory Barriers and Encouraging Investment and Training, DCPD-201500195 (Mar. 23, 2015), http://1.usa.gov/25yy7Ql.

better support the needs of communities seeking broadband investment."[32] The White House released the Council's report in 2015 outlining action items and milestones to be taken by each agency to remove barriers to broadband deployment.[33]

By focusing on accelerating the buildout of broadband infrastructure on federal lands, the government led by example, catalyzing investment and innovation in the private sector and forging many innovative public/private partnerships.[34] It can and should play a similar role here with respect to the deployment of infrastructure necessary to advance IoT technologies.

G. How Government Should Quantify and Measure the IoT Sector (Question 11); How Government Should Measure the Economic Impact of IoT (Question 12)

Our projections show that in 2016 alone, IoT applications will drive the consumer technology industry to $287 billion in retail revenues.[35] IoT also has significant potential to save consumers money and reduce residential energy consumption.[36] Although estimates vary, they all foretell incredible potential.[37] For example, ABI research forecast that IoT-related value

[32] NTIA, *Broadband Opportunity Council*, http://1.usa.gov/1Uf2qUz.

[33] Penny Pritzker and Tom Vilsack, Dept. of Commerce & U.S. Dept. of Agriculture, *Broadband Opportunity Council Report and Recommendations* (Aug. 20, 2015), http://1.usa.gov/1JlSS3V.

[34] See e.g., NTIA, *Broadband Technology Opportunities Program (BTOP) Quarterly Program Status Report* (July 2015), http://1.usa.gov/1t1JWRA; NTIA, *BroadbandUSA: An introduction to effective public-private partnerships for broadband investments* (Jan. 2015), http://1.usa.gov/1B7L9YD.

[35] CTA, *U.S. Consumer Technology Sales and Forecasts* (Jan. 2016), https://www.cta.tech/Research/Products-Services/Consumer-Sales-Forecast.aspx.

[36] Press Release, CTA, H*ome Automation, IoT Could Cut Energy Consumption 10 Percent, says CTA Study* (explaining that a recent study predicts that "widespread adoption of home automation products such as temperature, circuit and lighting control, if used for energy savings purposes, could collectively avoid up to 100 million tons of CO2 emissions and reduce total residential primary energy consumption by as much as 10 percent - that savings is more than consumer electronics' share of residential primary energy consumption (8.4 percent) according to a separate CTA study").

[37] *See, e.g.*, *Unlocking the Potential* ("If policy makers and businesses get it right, linking the physical and digital worlds could generate up to $11.1 trillion a year in economic value by 2025."); Louis Columbus, *Roundup Of Internet of Things Forecasts And Market Estimates, 2015*, Forbes (Dec. 27, 2015 3:39 PM) (surveying several IoT market forecasts), http://onforb.es/1ZbLjXD.

added services will grow from $50 billion in 2012 to $120 billion in 2018.[38] In a comprehensive study, Cisco predicted that the IoT will "create[] $14.4 *trillion* in Value at Stake—the combination of increased revenues and lower costs that is created or will migrate among companies and industries from 2013 to 2022."[39] Because IoT applications will become so entwined with everyday activity, the focus should be on the marginal benefit (and marginal cost) of IoT uses.

H. Impact of the Growth of IoT on the U.S. Workforce and Potential Benefits for Employees and/or Employers (Question 14)

Advances in the IoT, combined with general innovation-friendly policies, can help the U.S. maintain its role as a global leader in technology and unleash economic growth.[40] The U.S. technology sector is the strongest and most innovative in the world, and appropriate limited federal and state government action, as well as restraint, will ensure that the nation maintains its leadership in the burgeoning IoT market.[41] However, this leadership is being challenged by other countries that are aggressively pursuing IoT transformation. For example, China has stated that "Made in China 2025", the Chinese government's blueprint for overhauling industry and rebranding China as a high-quality manufacturer, is based on smart manufacturing (a network of intelligent, connected factories), emphasizes innovation and quality, and includes US$6.4 billion exclusively for China's emerging industries.[42] Additionally, Germany is actively pursuing Industrie 4.0, the German vision for the future of manufacturing, where smart factories use

[38] *Id.*

[39] Joseph Bradley, *Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion*, Cisco White Paper, at 1(2013), http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy.pdf.

[40] *See infra* Section II.N discussing tax and immigration policies that can increase these benefits.

[41] *See* Intel, *Policy Framework for the Internet of Things (IoT)* (2014) (describing the value to the U.S. economy of the U.S. tech sector taking a leading role in the global IoT market), http://intel.ly/22okUYy.

[42] Ringier Metalworking, *Smart Manufacturing in China*, industrysourcing (Sept. 5, 2015 11:09:23 AM), http://www.industrysourcing.com/article/smart-manufacturing-china.

information and communications technologies to digitize their processes and reap huge benefits in the form of improved quality, lower costs, and increased efficiency.[43] As CTA has observed:

> With some of the world's most disruptive companies - both global brands and innovative startups - the U.S. tech sector will help reduce the deficit, create jobs, improve sustainability and grow the economy. And tech's evolving sharing economy brings unique value, giving us more transportation and hospitality choices, creating good jobs with flexible hours and tapping capital resources such as a second car or a spare bedroom. But we must have the right policies in place to achieve tangible benefits.[44]

I. How Government Should Address the Main IoT Policy Issues (Question 15)

The RFC observes that a "growing dependence on embedded devices in all aspects of life raises questions about the confidentiality of personal data, the integrity of operations, and the availability and resiliency of critical services."[45] Yet while government has a critical role to play in ensuring that its policies enable industry to meet demand for IoT offerings, it must be sure to limit other types of regulatory intervention—and to forego entirely any actions that could stifle innovation in the nascent IoT ecosystem.[46] Prescriptive regulation, however well intentioned, could inadvertently deter the development and deployment of the IoT. Likewise, fragmented and, its flip-side, overlapping regulations are artificial hurdles that the Department should avoid. Specifically, policymakers at all levels of government should exercise regulatory humility, taking only actions consistent with the following core framework:

[43] Sara Zaske, *Germany's vision Industrie 4.0: The revolution will be digitized*, ZDNet (Feb. 23, 2015 08:33 GMT), http://www.zdnet.com/article/germanys-vision-for-industrie-4-0-the-revolution-will-be-digitised.

[44] Press Release, CTA, *Tech Innovation Key to President's SOTU Vision, Says Consumer Technology Association* (Jan. 12, 2016), http://cta.tech/News/News-Releases/Press-Releases/2015-Press-Releases/Tech-Innovation-Key-to-President-s-SOTU-Vision,-sa.aspx.

[45] RFC at 19,959.

[46] For example, the hands-off approach to Internet regulation launched massive innovation. The Department should replicate that approach with the IoT.

First, to promote innovation, policymakers should favor market-based solutions over prescriptive regulations. Government should apply regulation only if there is a compelling public interest in doing so.[47] Policymakers should not reflexively second-guess how consumers or businesses decide to incorporate technology into their lives. Likewise, in the rare event where policymakers believe that regulation would be superior to a market-based outcome, policymakers should test their assumption by applying empirical analyses to do a comprehensive cost-benefit analysis vis a vis alternative technologies, as well as determine whether the benefits of a proposed regulatory mandate will exceed its costs. Such cost-benefit analyses can help balance the need for consumer protection with the need to allow flexibility to innovate.[48] Independent industry data should play a key role in these decisions.

Second, the primary goal of any IoT policy regime should be to promote innovation. As President Barack Obama observed in his 2011 State of the Union address: "The first step in winning the future is encouraging American innovation…. [W]hat America does better than anyone else … is spark the creativity and imagination of our people…. In America, innovation

[47] *See* Gary Shapiro, *How the Heavy Hand of Government Stifles the On Demand Economy*, TechDirt (Aug. 25, 2015) ("*The Heavy Hand of Government*"), https://www.techdirt.com/articles/20150824/11370432049/how-heavy-hand-government-stifles-demand-economy.shtml.

[48] For decades, Executive Branch agencies in the United States have been required to "(1) propose or adopt a regulation only upon a reasoned determination that its benefits justify its costs (recognizing that some benefits and costs are difficult to quantify); (2) tailor [their] regulations to impose the least burden on society, consistent with obtaining regulatory objectives, taking into account, among other things, and to the extent practicable, the costs of cumulative regulations; (3) select, in choosing among alternative regulatory approaches, those approaches that maximize net benefits (including potential economic, environmental, public health and safety, and other advantages; distributive impacts; and equity); (4) to the extent feasible, specify performance objectives, rather than specifying the behavior or manner of compliance that regulated entities must adopt; and (5) identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, such as user fees or marketable permits, or providing information upon which choices can be made by the public." *See* Exec. Order No. 13, 563, 76 Fed. Reg. 3,821 (Jan. 18, 2001) (summarizing Exec. Order No. 12,866, 58 Fed. Reg. 51,735 (Sept. 30, 1993)). President Obama enhanced these principles, directing agencies to, among other things, "identify and consider regulatory approaches that reduce burdens and maintain flexibility and freedom of choice for the public" where permitted by law.

doesn't just change our lives. It is how we make our living."[49] Further, "our free enterprise system is what drives innovation."[50]

Third, if policymakers decide that some form of oversight is appropriate in a given case, they should proceed with caution, favoring self-regulation over command-and-control on determining how the outcomes are achieved. CTA and groups like it have long been committed to solutions that marry industry expertise, stakeholder involvement, and the flexibility required by a fast-changing marketplace. Standards ensure that technical issues are addressed in cooperative forums, principally by technologists rather than attorneys, and often eliminating any need for regulatory mandates. A wide variety of groups develop and enforce tailored industry codes of conduct that hold bad actors to account without undermining innovation.[51]

Consistent with these principles, policymakers should reject mandates that would distort the IoT's trajectory and undercut the growth of offerings that would expand consumers' welfare. In particular, they should reject actions that favor one platform or technology over another or create or expand uncertainty, and should foreswear excessively punitive enforcement penalties.[52] In the case of the IoT, incorrect, unnecessary, or premature mandates have the potential to distort the marketplace in a way that may disadvantage the US on a globally competitive basis. They could delay, dis-incentivize or prevent the development of new and superior technologies that would do better to improve our health outcomes, energy conservation efforts, or highway safety (to take just three examples). While protection of consumers should always remain at the forefront of regulators' minds, government must refrain from over-reaching enforcement actions

[49] The White House, *Remarks by the President in State of Union Address* (Jan. 25, 2011), http://1.usa.gov/1Uisr5d.

[50] *Id.*

[51] *See infra* Section II.J, responding to Questions 16-17.

[52] *See The Heavy Hand of Government*.

that harm consumers by mandating a specific technology, increasing the cost of providing service or entering a sector without providing commensurate consumer benefit.

J. How Government Should Address IoT Cybersecurity and Privacy Concerns (Questions 16-17)

The Internet's growth is largely attributable to the success of consensus-driven stakeholder processes to address policy issues,[53] and the privacy and security concerns associated with the IoT closely mirror those in which industry already has a strong track record of developing and implementing best practices to protect consumers. To address cybersecurity and privacy concerns, government must continue to foster industry-wide, consensus-driven self-regulation that is nimble and keeps pace with rapidly evolving technologies.

Self-regulatory regimes have worked well to ensure consumer privacy and foster innovation. The use of consumer information for marketing and other purposes is not new, as marketers have engaged in responsible collection of data for more than 100 years.[54] Time and again, industry has proactively addressed emerging privacy and security issues.[55] In contrast,

[53] *See, e.g.*, *Executive Office of the President of the United States, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 23 (2012) ("the Administration believes that multistakeholder processes underlie many of the institutions responsible for the Internet's success"), http://1.usa.gov/1FQW1XF ("Consumer Data Privacy Framework").

[54] Susan Taplinger, *The Plain Facts: Why Self-Regulation Works Better than Government Regulation*, DMA (May 9, 2014), http://thedma.org/blog/advocacy/the-plain-facts-why-self-regulation-works-better-than-government-regulation.

[55] Efforts of organizations like the Digital Advertising Alliance and Network Advertising Initiative have provided robust protections and tools to consumers as they use the Internet. *See, e.g.*, Consumer Data Privacy Framework, *supra*, at 12-13 (citing AboutAds.info, Self-Regulatory Principles for Online Behavioral Advertising (July 2009)) ("[P]rompted by the FTC, members of the online advertising industry developed self-regulatory principles based on the FIPPs, a common interface to alert consumers of the presence of third party ads and to direct them to more information about the relevant ad network, and a common mechanism to allow consumers to opt out of targeted advertising by individual ad networks."), http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf; Edith Ramirez, Chairwoman, FTC, *Cross-Device Tracking: An FTC Workshop*, 6-7 (Nov. 16, 2015) ("The Digital Advertising Alliance and the Network Advertising Initiative have also taken steps to enhance privacy protections in the online advertising space. The organizations' self-regulatory principles encourage

unnecessary government action can skew or suppress innovation, create market uncertainty, and ultimately harm consumers. Legislation and regulation often fail to keep up with ever-evolving technology, and often rely—to the detriment of the marketplace and consumers—on regulators' static assumptions and predictions of where the market is going and what consumers want. Self-regulation is nimble, and can be more easily updated to address changes in the marketplace and technology. And self-regulatory efforts push companies to "internalize ethical behavior and principles since the rules are based on social norms and conduct of peers rather than top-down prescriptive rules."[56] In fact, self-regulatory codes may be the *best* way to effectuate consumer adoption of the IoT.[57] As a backstop with respect to consumer privacy, the FTC can utilize its Section 5 authority to protect against any privacy-related practices that are unfair or deceptive.[58]

As a general matter, the increasing number of devices should not automatically trigger new regulations—before acting, there should be evidence of real harms. As IoT standards and technology continue to develop, regulatory efforts should be designed to promote innovation and

members to provide increased transparency and offer consumers control over data collection for certain practices. DAA and NAI also have developed useful opt-out tools for online data collection covered by their self-regulatory codes. NAI has also issued guidance relating to the use of non-cookie technologies, emphasizing that members should honor user opt-outs regardless of the technology used. NAI is currently developing and testing a new centralized opt-out tool that will inform consumers when NAI members use non-cookie technologies for interest-based advertising."), http://1.usa.gov/1XvgbU6.

[56] Daniel Castro, *Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising*, The Information Technology & Innovation Foundation, 6 (Dec. 2011), http://www.itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf.

[57] Christopher Wolf and Jules Polonetsky, *An Updated Privacy Paradigm for the "Internet of Things"*, The Future of Privacy Forum, 11 (Nov. 19, 2013) ("As the Internet of Things becomes more ubiquitous, parents will want to control what can be done with information collected from devices associated with their children. Others may want to indicate their preferences about how third-party connected devices will communicate with them. Self-regulatory codes of conduct will be the most effective means to honor these preferences and others in the rapidly evolving landscape of the Internet of Things."), https://fpf.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-%E2%80%9CInternet-of-Things%E2%80%9D-11-19-2013.pdf.

[58] In addition the FTC action, the Department should note that regulations already exist and apply to IoT with respect to privacy, data security, energy, finance, and transportation.

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

Moreover, the Department should note that stakeholders already are proactively addressing IoT privacy concerns.[59] In addition, CTA and its members participate in a number of other ongoing efforts to address a host of IoT issues, including those convened by think tanks, other associations, and the Administration.[60] Other examples include:

- The Future of Privacy Forum's discussion document on privacy principles for facial recognition technology;[61]

- The President's National Security Telecommunications Advisory Committee ("NSTAC"), with the mission to provide the U.S. Government the best possible industry advice in areas of national security;[62]

[59] For example, in early 2015, CTA began a process to establish a first-of-its-kind set of voluntary guidelines for private sector organizations that handle personal wellness data, which often is generated by wearable technologies. The process culminated in CTA's October 2015 announcement of the Guiding Principles on the Privacy and Security of Personal Wellness data, which establish a baseline, voluntary framework to promote consumer trust in technology companies. Among other things, the Guiding Principles recommend that companies: provide robust security measures; provide clear, concise, and transparent information on the use of data collection, storing, and sharing, especially when transferring data to unaffiliated third parties; allow consumers the ability to control and review their personal wellness data; offer users the ability to opt out of advertising; and disclose their protocol for responding to law enforcement requests. *See* CTA, *Guiding Principles on the Privacy and Security of Personal Wellness Data*, http://www.cta.tech/healthprivacy; CTA, *Association Unveils First-of-Its-Kind, Industry Supported Principles on Wellness Data Privacy* (Oct. 26, 2015), https://www.cta.tech/News/News-Releases/Press-Releases/2015-Press-Releases/Association-Unveils-First-of-Its-Kind,-Industry-Su.aspx. CTA intends to review the Guiding Principles with members on a regular basis to ensure that the Principles accurately reflect current data privacy and security concerns.

[60] For example, the National Cyber Security Alliance and the WiFi Alliance, both of which share some members with CTA, have developed the following resources: http://www.StaySafeOnline.org and http://www.wi-fi.org/discover-and-learn/security.

[61] The Future of Privacy Forum, *Privacy Principles for Facial Recognition Technology* (Dec. 2015), https://fpf.org/wp-content/uploads/2015/12/Dec9Working-Paper-FacialRecognitionPrivacyPrinciples-For-Web.pdf.

[62] *See* Department of Homeland Security, *About NSTAC*, https://www.dhs.gov/about-nstac.

- The Alliance of Automobile Manufacturers and the Association of Global Automakers' initiative to establish privacy principles;[63]

- The Automotive Security Review Board initiative to codify best practices and design recommendations for advanced cybersecurity solutions and products to benefit the automobile industry and drivers;[64]

- The Online Trust Alliance's IoT Trust Framework, which currently includes practices to address security, privacy, and sustainability concerns in connected home products and consumer-facing wearable technologies;[65] and

- The NTIA's multistakeholder process to develop privacy, transparency, and accountability best practices for unmanned aircraft system use.[66]

K. Ways that the IoT Affects and is Affected by Questions of Economic Equity (Question 19)

In addition to improving government services and increasing industrial efficiency, IoT applications have the potential to provide critical services for all Americans, including members of "disadvantaged communities and groups" and rural communities.[67] For example, CTA's research demonstrates that the IoT applications can "prevent and preempt life inconveniences caused by … aging challenges."[68] As the aging population increases, institutional long-term care services cannot meet demand and, even if they could, many seniors want to age in their homes for as long as possible.[69] Emerging applications include safety monitoring that can prevent

[63] The Alliance of Automobile Manufacturers, Automotive Privacy: Automakers Believe that Strong Consumer Data Privacy Protections are Essential to Maintaining the Trust of Our Customers, http://www.autoalliance.org/auto-issues/automotive-privacy.

[64] The Automotive Security Review Board, https://newsroom.intel.com/news-releases/intel-commits-to-mitigating-automotive-cybersecurity-risks.

[65] Online Trust Alliance, *Internet of Things*, https://otalliance.org/initiatives/internet-things.

[66] NTIA, *Multistakeholder Process: Unmanned Aircraft Systems*, http://1.usa.gov/1KQNZYy.

[67] RFC at 19,959 ("In what ways could IoT potentially help disadvantaged communities or groups? Rural communities?").

[68] Consumer Technology Association Foundation and CTA, *Active Aging Study*, Report, at 6 (Mar. 2016).

[69] *Id.* at 66-68; Steven Ewell, *Smart Homes for Long Lives*, CTA i^3 ,at 46 (Sept./Oct. 2015) (also noting that programs, such as the CTA Foundation-supported Selfhelp Virtual Senior Center, is "using technology to reconnect homebound seniors"), http://mydigimag.rrd.com/publication/?i=272619&p=48.

seniors from getting lost, improved living comfort through smart sensors and controls, and health monitoring can help seniors stay in their homes longer by making homes a little friendlier and reducing the time caregivers and even medical professionals need to spend on-site.[70] CTA Foundation proudly supports the Older Adults Technology Services' ("OATS") Senior Planet Exploration Center in New York, among many other initiatives, which offers classes and sits down with seniors to explain technologies, demystifying and unlocking technology.[71]

Similarly, individuals with disabilities—including many seniors—are harnessing the IoT to live safer, more independent lives:

> While many drivers dream about being able to sit back and relax during a long commute, [self-driving cars] can literally open a new world to those who are physically unable to drive, providing access to daily routines such as grocery shopping or visiting friends and family, as well as bigger opportunities like facilitating steady employment and accessing health care.[72]

For those with physical limitations, controlling lights and thermostats can transform a dwelling into a comfortable home.[73] IoT applications convert signals delivered aurally—think a doorbell and telephone ring—into signals delivered into visually or physical—flashing lights and

[70] *Id.* at 6.

[71] *See, e.g.*, CTA Foundation, Initiatives ("CTA Foundation Initiatives"), http://www.cta.tech/Foundation/Initiatives.aspx; *see also* CTA Foundation Initiatives (quoting a Senior Planet member, "This week I was awarded my 100th Elance job! I have retained my five-star average, and now have six repeat clients, and my latest ranking as of last week is No. 76 out of the 239,000 writers registered with the site worldwide. Prior to my OATS training, I had never even heard of Elance, but through your classes I gained the skills and confidence to give it a try.").

[72] CTA, *2015 Sustainability Report: Innovating a Better World*, at 44 (2015) ("*Innovating a Better World*"), http://content.ce.org/SReport2016/CTA_SR_2016/report-builder/_pdf/CTA_2015_SR.pdf.

[73] *See, e.g.*, Shalene Gupta, *For the disabled, smart homes are home sweet home*, Fortune (Feb. 1, 2015 6:00 AM EDT) ("For years, [Steve O'Hear, who uses an electrical wheelchair,] had to rely on someone else to turn the lights on–that is until he installed Internet-connected lights that he could turn on with his smartphone."), http://fortune.com/2015/02/01/disabled-smart-homes.

vibrating phones.[74] And, for individuals with cognitive disabilities, sensors can remind individuals to perform daily tasks or alert remote caregivers about a delayed routine task.[75] Importantly, many Consumer IoT applications are able to interface through smartphones, tablets, and other mobile devices, which have built in accessibility features for app designers and consumers to use. Finally, IoT-powered efficiency gains can lead directly to lower utility bills. A private-public partnership to ensure these communities have access to IoT devices can spur these benefits.

L. Factors and Issues the Department Should Consider in its International Engagement (Questions 20-23)

CTA commends the NTIA for separately soliciting comment in preparation for the upcoming 2016 World Telecommunications Standardization Assembly.[76] The Department should continue to solicit public comment on government positions in international standards fora.[77] With an extensive Technology and Standards program that includes more than 70 committees, subcommittees and working groups and roughly 1,100 participants as well as American National Standards Institute accreditation, CTA is a champion of voluntary, consensus-based standards. To that end, the Department, including NIST and NTIA, should promote international harmonization of standards. However, that harmonization should not be in the form of mandates from international fora. Further, the Department should continue to

[74] In particular, the CTA Foundation is partnering with the Gallaudet University Technology Access Program to use IoT to enable alerts for people are deaf or hard of hearing.

[75] *Innovating a Better World* at 44.

[76] *Input on Proposals and Positions for 2016 World Telecommunications Standardization Assembly*, Request for Public Comment, Docket No. 160509408-6408-01, RIN 0660-XC026, 81 Fed. Reg. 30518 (May 17, 2016) ("WTSA-2016 RFC"). CTA looks forward to commenting on the WTSA-2016 RFC.

[77] RFC at 19,958 ("Both NIST and NTIA have been actively engaged with international standards bodies and international organizations on aspects of IoT and other related areas (e.g., cybersecurity), and have been further engaged with other Federal agencies.").

promote regulatory harmonization to increase economics of scales. Consumers and society benefit when CTA's members are able to design, build, and test *once* and sell *everywhere*.

M. IoT Policy Areas that Could be Appropriate for Multistakeholder Engagement; Role the Department of Commerce Should Play in Addressing IoT Challenges and Opportunities and Collaborating with Stakeholders; Government and Private Sector Collaboration to Ensure that Infrastructure, Policy, Technology, and Investment are Working Together to Fuel IoT Growth and Development (Questions 25-27)

Building a strong public sector/private sector partnership can help bolster the foundation for consumer confidence and trust in the IoT. Government can advance the IoT by working with industry to develop a system of trust between users and connected things. Together government and industry can work to educate consumers on issues such as how to limit risks associated with unsecured connected devices (*e.g.*, by changing default passwords, using password-protecting home Wi-Fi networks, and employing virtual private networks).[78]

The public/private partnership that has coalesced around the Department's recent cybersecurity initiatives is particularly illustrative. Most notably, various critical infrastructure sectors came together to develop the NIST Cybersecurity Framework, a voluntary, flexible, and non-regulatory approach that enables companies of all types and sizes to tailor their cybersecurity efforts to meet their business models, infrastructure, and assets.[79] Similar

[78] One example of this is the FTC's groundbreaking "Start with Security" series, where the FTC has taken business guidance on the road to San Francisco, Seattle, and Austin, to meet with startups, experts, and agency officials to discuss effective data security strategies.

[79] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, NIST, 1 (Feb. 12, 2014) (explaining that the "[f]ramework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses"), http://1.usa.gov/1dIqXf5. In response to requests for comment by NIST, industry recently voiced continued support of the Cybersecurity Framework as companies work through the early phases of building it into their risk management processes. *See Views on the Framework for Improving Critical Infrastructure Cybersecurity*, 80 Fed. Reg. 76,934 (Dec. 11, 2015).

business-led collaboration continues through other established mechanisms.[80] Additional industry coordination is facilitated through the Communications Security, Reliability and Interoperability Council ("CSRIC")—an advisory committee to the FCC that recommends best practices and potential actions to ensure optimal security, reliability, and interoperability of commercial and public safety communications systems.[81] Concurrently, NTIA has used its multistakeholder processes to further catalyze industry discussion on the cybersecurity-related issues, with the stated goal of avoiding regulatory solutions.[82] Of course, all of these efforts parallel industry's own initiatives, such as the Building Security in Maturity Model ("BSIMM")—a study of actual software security initiatives that likewise is not a one-size-fits-all prescription.[83] In short, cybersecurity issues are being addressed in a multi-layered fashion, with industry consistently taking a lead in shaping the discussion. A similar approach to challenges posed by the growth of the IoT would ensure protection of consumers' safety and quality of

[80] *See, e.g.*, *About CSCC*, U.S. Communc'ns Sector Coordinating Council, (describing means of coordination used by the Communications Sector Coordinating Council), http://www.commscc.org/about. Sector Coordinating Councils formed for each of sixteen critical infrastructure sectors.

[81] *See The Communications Security, Reliability and Interoperability Council*, FCC, http://transition.fcc.gov/pshs/advisory/csric. CSRIC's working groups have proposed implementation guidance to help communications companies implement the NIST Cybersecurity Framework and continue to recommend and refine best practices in this space. *Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report*, CSRIC IV (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[82] *See, e.g.*, *Stakeholder Engagement on Cybersecurity in the Digital Ecosystem*, 80 Fed. Reg. 14,360, 14,363 (Mar. 19, 2015) (recognizing that traditional regulation in this context is "difficult and inefficient" in light of the "pace of innovation in the highly dynamic digital ecosystem"); *id.* at 14,365 (stating that "[i]n the digital ecosystem, the rapid pace of innovation often outstrips the ability of regulators to effectively administer key policy questions," and that "[o]pen, voluntary, and consensus-driven processes can work to safeguard the interests of all stakeholders while still allowing the digital economy to thrive"); Angela Simpson, Deputy Assistant Sec'y of Commerce for Commc'ns and Info., Nat'l Telecomm. & Info. Admin., Remarks at the Vulnerability Research Disclosure Multistakeholder Process (Sept. 29, 2015) ("it is not our job to tell you what to do. NTIA will not impose its views on you. We will not tip the scales. We are not regulators. We are not developing rules. We do not bring enforcement actions. Instead, we are in a unique position to encourage you to come together, to cooperate, and to reach agreement on important issues."), http://1.usa.gov/1XvgMFd.

[83] *About BSIMM*, Building Security in Maturity Model, https://www.bsimm.com/about.

service, while affording industry the opportunity to directly participate and shape parameters that can evolve flexibly as new business and technological developments emerge.

N. Additional Relevant Issues (Question 28)

The government can take additional steps toward ensuring that the U.S. IoT ecosystem maintains its global leadership role. For example:

Demand Stimulation**.** The government can generate demand for IoT technologies, which will help jumpstart the development of the IoT ecosystem. Agencies can utilize IoT technology themselves to increase efficiency in their management of public infrastructure and also can incent or require regulated utilities to use IoT technologies to more efficiently manage and conserve regulated resources such as energy and water.[84] This will result in direct and immediate benefits to the American public while simultaneously stimulating the IoT markets that supply the government and public utilities. By making the data collected by government-operated IoT systems available to industry (subject to appropriate privacy safeguards), governments can enable private companies to independently develop innovative new market niches. Through private-public partnerships, governments can empower private companies to develop new and better ways for governments to utilize IoT-generated data to provide more efficient and desirable public services.

Tax**.** Tax policy can help facilitate the rapid growth of the IoT sector, as exemplified by recent federal legislation making permanent certain previously temporary research and development ("R and D") tax credits. Federal and state R and D tax credits reduce the risk to companies of investment in basic and applied R and D. Reduced risk fosters greater investment, which in turn spurs the type of rapid technological advancement that is predicted for the IoT

[84] *See, e.g.*, *supra* Section II.F (discussing the Smart Cities Initiative).

sector over the next decade. The U.S. government took a strong step in the right direction when it expanded and made permanent the federal R and D tax credit in December 2015.[85] However, there remains room for improvement. In addition, more attention needs to be given to the unintended consequences of tax policies on the IoT market. Tax laws should foster IoT innovation rather than providing disincentives to the continued rapid deployment of the IoT, which should be driven by competition and consumer demand.

***Immigration*.** Appropriate immigration policies are key to unleashing the potential of the IoT sector. In light of the breathtaking growth expected in this sector over the next decade, it is unlikely that the U.S.'s science, technology, engineering, and math ("STEM") work force will be sufficient to support the sector's rapid expansion[86] unless Congress adopts meaningful reform to the U.S.'s overly restrictive immigration policies. Strategic immigration reforms are needed to encourage U.S.-educated immigrants to remain in the U.S. to build businesses and create domestic jobs, and U.S. immigration policy should proactively promote their participation.

[85] Consolidated Appropriations Act, P.L. 114-113 § 1, 114th Cong. (2015) (Protecting Americans From Tax Hikes Act of 2015 was consolidated with the Military Construction and Veterans Affairs and Related Agencies Appropriations Act, H.R. 2029 (2016)). The PATH Act made permanent the R and D tax credit that initially was established in 1981and that has expired and been renewed more than a dozen times since then. The law provides companies with a tax credit of up to 20% of their qualifying research expenditures. The PATH Act also enacted changes to the application of the credit, which increased its effective availability to small and medium-sized businesses. *Id.*

[86] Adams B. Nager and Robert D. Atkinson, *Debunking the Top Ten Arguments Against High-Skilled Immigration*, Information Technology & Innovation Foundation (Apr. 2015), http://www2.itif.org/2015-debunking-myths-high-skilled.pdf?_ga=1.42898860.847894678.1456315207.

III. CONCLUSION

The U.S. has a chance to harness the opportunities of the IoT to bring significant consumer, business, and societal benefits to the nation and solidify our global leadership in technology innovation and deployment. Policymakers should aggressively accelerate the positive steps government can take to promote IoT innovation, growth, and deployment, such as making more spectrum available and harmonizing federal agency interaction, and refrain from broad regulatory action that would derail or delay new IoT technologies. Self-regulatory and other consensus-driven industry efforts allow stakeholders to address discrete, specialized issues that may arise in a practical and flexible manner and without the same risks to competition and innovation—and these should be the default institutional mechanism for the IoT. For the IoT to flourish generally—and for new, never-thought-of-before IoT applications to positively impact and improve our lives—government must partner with industry to eliminate barriers to innovation, exercise regulatory humility by considering any regulatory actions in light of greater economic impacts, and embrace industry self-regulatory efforts that can address concerns as they arise without inhibiting innovation.

Respectfully submitted,

CONSUMER TECHNOLOGY
ASSOCIATION F/K/A CONSUMER
ELECTRONICS ASSOCIATION

By: *\/s/ Julie M. Kearney*

Julie M. Kearney
Vice President, Regulatory Affairs
Alexander B. Reynolds
Director, Regulatory Affairs
Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7644

June 2, 2016