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. 170105023-7023-01
	)	
	)	
	)	

COMMENTS OF THE CONSUMER TECHNOLOGY ASSOCIATION

CONSUMER TECHNOLOGY ASSOCIATION

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

March 13, 2017

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. 170105023-7023-01
	)	
	)	

COMMENTS OF THE
CONSUMER TECHNOLOGY ASSOCIATION

I. INTRODUCTION

The Consumer Technology Association ("CTA")[1] stands for innovators, including the numerous companies – from large household names to entrepreneurial startups – whose products and services largely comprise the Internet of Things ("IoT"). Representing an industry responsible for supporting more than 15 million U.S. jobs and generating more than $290 billion in revenue in the U.S., CTA looks forward to continuing to work with the Department of Commerce ("Department") and the new Administration on efforts to promote and further expand the IoT as an engine for U.S. job creation and technological and economic leadership. CTA is pleased to provide comments on the Department's January 12, 2017 "Green Paper" on fostering the advancement of the Internet of Things.[2] As CTA's comments explain, the Green Paper sets

---

[1] The Consumer Technology Association (CTA)™ is the trade association representing the $292 billion U.S. consumer technology industry, which supports more than 15 million U.S. jobs. 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 technologies. Profits from CES are reinvested into CTA's industry services.

[2] Department of Commerce, Fostering the Advancement of the Internet of Things (Jan. 2017) ("Green Paper"), https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf. CTA provides its comments in response to the Request for Comment that the National Telecommunications and Information Administration ("NTIA") issued in connection with the Green Paper. The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of

forth several key ideas that, if implemented, would encourage the rapid and broad adoption of IoT technologies by American businesses, government, and citizens.[3]

Advances in the IoT, combined with innovation-friendly policies, can help the U.S. unleash economic growth and maintain its global leadership role in technology, including the burgeoning IoT market.[4] To maintain this position, however, the United States needs to change its recent course of burdensome regulation. Since 2009, federal regulators have issued more than 20,000 rules,[5] increasing regulatory compliance costs by over $100 billion annually.[6] Small businesses, including tech startups, shoulder a disproportionate share of the burden. As CTA consistently has said, government must allow consumers and the market to decide IoT winners and losers, rather than dictate a specific technology solution. This is particularly critical in a nascent market like the IoT, where products and services are in early stages, insight into consumer preferences are just beginning to take shape, and business models are still in flux. Overly broad and prescriptive rules, even when well intended, can inadvertently throttle innovation, prevent beneficial new products from coming to market, and inhibit security innovations that would promote safety. When agencies attempt to proactively resolve problems

---

Things, 82 Fed. Reg. 4313 (Jan. 13, 2017), https://www.gpo.gov/fdsys/pkg/FR-2017-01-13/pdf/2017-00720.pdf.

[3] As Commerce Secretary Wilbur Ross stated in his confirmation hearing, all parties with an interest in the Internet of Things "need encouragement." Commerce Secretary Confirmation Hearing, C-SPAN (Jan. 18, 2017), https://www.c-span.org/video/?421257-1/commerce-secretary-nominee-wilbur-ross-testifies-confirmation-hearing.

[4] *See* Comments of CTA, Docket No. 1603311306-6306-01 (RIN 0660-XC024), at 2 (June 2, 2016) ("CTA Initial Comments"), https://www.ntia.doc.gov/files/ntia/publications/cta_comments_re_ntia-_iot_rfc-final-060216_2.pdf.

[5] *See* Maeve P. Carey, Congressional Research Service, *Counting Regulations: An Overview of Rulemaking, Types of Federal Regulations, and Pages in the Federal Register*, at 5-6 (Oct. 4, 2016), https://fas.org/sgp/crs/misc/R43056.pdf (listing number of final rules issued by year).

[6] *See* James Gattuso & Diane Katz, Heritage Foundation, *Red Tape Rising 2016: Obama Regs Top $100 Billion Annually* (May 23, 2016), http://www.heritage.org/government-regulation/report/red-tape-rising-2016-obama-regs-top-100-billion-annually.

by regulating hypothetical harms, they inevitably choke innovation and unintentionally favor incumbent players with old technologies and standards. Instead, the government should only consider regulating in response to concrete and substantial harms, and then only with technology-neutral policies that do not put disruptive technologies at a disadvantage.[7]

At this stage, bipartisan working groups in the House and Senate, as well as the IoT Caucus, have recognized that the key policy task is to ensure federal policy spurs the innovation economy, while also promoting security and protecting consumers. The Green Paper identifies appropriate priorities along these dimensions, including enabling access to additional flexible-use spectrum; promoting global industry-led standards development (*e.g.*, to support global IoT interoperability); and encouraging the growth and development of open and competitive markets. The Green Paper also suggests a role for the Department in crafting balanced policy and building coalitions on issues such as cybersecurity, privacy, and intellectual property. CTA applauds the Department for identifying these key areas for collaboration and urges the Department to focus on coalition building, public-private partnerships, and industry self-regulation, rather than recommending prescriptive rules. The Green Paper principles generally favor such a targeted, hands-off approach, including reliance on industry-driven, consensus-based, voluntary standards; reducing barriers to entry; and convening stakeholders to address public policy challenges. This is also the best way to encourage privacy and security standards that apply consistently across the digital economy – for the IoT and other connected technologies. By addressing new technologies with this smart and light-touch regulatory approach, the government will empower business leaders to invest time and resources into growing their companies, creating high paying

[7] Gary Shapiro, *Congress: Want America to Innovate? We Need Smart Regulation*, medium.com (Feb. 1, 2017) ("Shapiro, *Want America to Innovate?*"), https://medium.com/@GaryShapiro/congress-want-america-to-innovate-we-need-smart-regulation-4b760e57c91e#.ifh8xl23b.

new U.S. jobs, and developing new products and services that will change Americans' lives for the better.[8]

II. RESPONSES TO RFC QUESTIONS

A. Is the discussion of IoT in the Green Paper regarding the challenges, benefits, and potential role of government accurate and/or complete, and are there issues that were missed or should be reconsidered?

The Green Paper clearly demonstrates that the Department recognizes the infinite possibilities of the IoT to improve the operations of U.S. companies, enhance the public services provided by all levels of government, and augment and reshape the lives of American citizens.[9] It discusses the many gains in efficiency, productivity, quality, and safety that the IoT will bring to a broad range of industries, including manufacturing, healthcare, transportation, energy, and retail, and finds that consumers will see benefits through smart homes, vehicle automation, and other connected devices. The Green Paper also notes that the IoT may enable governments to deliver better, cheaper, and more efficient public services, including safety and security services. CTA appreciates the Department's statement that IoT technologies "promise a wide array of safety and efficiency benefits for consumers and businesses alike"[10] and encourages the Department to continue to stay abreast of new IoT technologies and business models as they rapidly evolve. CTA would be pleased to assist in this regard at the Department's request.

The Green Paper concludes that the challenges and opportunities presented by the IoT require a reaffirmation, not a reevaluation, of the well-established U.S. government policy approach to emerging technologies (*e.g.*, encouraging private sector leadership and global

[8] *See id.*

[9] Green Paper at 8-10.

[10] *Id.* at 8.

standards development, and using a collaborative multistakeholder approach to policy making).[11] This is the right conclusion. As CTA has explained, one of the most significant challenges to U.S. IoT leadership is the existing fragmented approach of federal government agencies toward its development, resulting in inconsistent and reactive policy and regulatory regimes.[12] Toward this end, CTA supports the DIGIT Act, which would give the Department the lead responsibility in identifying regulatory and other barriers to IoT development.[13] Thus, as the Green Paper finds, coordination among U.S. government partners would be helpful due to the complex, interdisciplinary, cross-sector nature of IoT and may also be useful when working with international and private sector partners.[14] The Green Paper correctly concludes that the government will need to maintain its robust advocacy for industry-led approaches and consensus-based standards on the global stage and should continue to use multistakeholder approaches.[15] To do so, as the Green Paper notes, the Department can look to its successful efforts to date in building flexible and adaptable frameworks, codes of conduct, and best practices.[16] CTA further encourages government to invest in these multistakeholder efforts, as the IoT continues to evolve.

---

[11] The Green Paper correctly focuses on scope (IoT connects a wider range of systems and devices than ever before), scale (the magnitude of connected devices), and stakes ("A major internet outage or a cyberattack would never have been without consequence, but IoT raises the stakes significantly, as such events can now affect medical devices, supply chain reliability, and cars driving down the highway, raising the real possibility of physical harm."). *Id.* at 4 (citation omitted).

[12] *See* CTA Initial Comments at 4.

[13] For further discussion of the DIGIT Act, see *infra* section II.D.

[14] Green Paper at 10-13. CTA encourages the Department to continue including digital economy issues in its formal government-to-government dialogues with top trading partners and to support continued IoT engagement internationally.

[15] *Id.* at 11.

[16] *Id.* at 12-13.

B. Is the approach for Departmental action to advance the IoT comprehensive in areas of engagement, and where does the approach need improvement?

Consistent with CTA's initial comments, the Green Paper sets forth Departmental priorities that include enabling access to flexible-use spectrum, promoting global standards and technology advancement, and encouraging markets (for example, through public-private partnerships and workforce education and training).[17] CTA applauds the Department for recognizing the "significant role" wireless technologies will play in supporting connected devices, with IoT apps "leverag[ing] . . . 5G [ ] technologies, innovative unlicensed use of spectrum, and low-power connectivity protocols, among other advances," and for understanding that a "shortage of available spectrum could become a constraint on the growth of IoT."[18]

Indeed, to connect the tens of billions of devices expected to be in use by 2020, some estimates suggest that networks 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 the U.S. economy, a broad range of agencies must coordinate amongst themselves and partner with industry to ensure sufficient spectrum for the IoT. The wide variety of IoT spectrum uses means that NTIA must help facilitate sharing or clearing of federally controlled spectrum. Given the cross-cutting nature of IoT, agencies must collaborate to enable the IoT to flourish. As Commerce Secretary Wilbur Ross said at his confirmation hearing, "[w]e need more spectrum in the private sector, and I will try my best to help convince those government agencies that have spectrum and don't

---

[17] *See* CTA Initial Comments at 15-16.

[18] Green Paper at 16-18.

[19] *See* CTA Initial Comments at 9 (citing Murray Slovick, *5G: The Mobile Tech of 2020*, CONSUMER ELECTRONICS ASSOCIATION I[3], 20, 22 (Nov./Dec. 2014), http://cdn.coverstand.com/25838/232265/-711ba5485b2b1c66036f89c895b2baecbaa98e91.23.pdf).

really need it to permit it to be commercialized."[20] He appropriately concluded that while we cannot compromise national defense, we must be rational and combat spectrum hoarding. This is especially true where exclusive spectrum was allocated over a decade or more ago and it is possible that today's technology advancements can enable efficient spectrum sharing.

Although opening additional licensed and unlicensed spectrum for new innovation, including innovation based on new, globally harmonized technologies like 5G, will be foundational to promoting the growth of the IoT, there is a broader and more significant infrastructure objective if America is to lead the world for decades to come: Government must incentivize cutting-edge IoT solutions to advance the Administration's broader infrastructure rebuilding and development goals – by incorporating smart technologies into public infrastructure projects. 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."[21] CTA encourages the Department to pursue the next steps proposed in the Green Paper, including coordinating with private sector, federal, state, and local government partners to ensure infrastructure continues to expand and remains innovative, open, secure, interoperable, and scalable.[22] CTA looks forward to engaging with the Department on these efforts to leverage "smart," forward-looking solutions in the nation's transportation, energy, and security

[20] Amir Nasr, *Here's What Ross Said About Tech Policy During His Confirmation Hearing*, Morning Consult (Jan. 18, 2017), https://morningconsult.com/2017/01/18/heres-ross-said-tech-policy-confirmation-hearing (Testimony of Wilbur Ross).

[21] The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, 81 Fed. Reg. 19956, 19959 (Apr. 6, 2016) ("RFC"), https://www.gpo.gov/fdsys/pkg/-FR-2016-04-06/pdf/2016-07892.pdf.

[22] Green Paper at 23-24.

infrastructure, as well as opportunities to invest in infrastructure that will accelerate U.S. leadership in innovative technologies like autonomous vehicles.

The Green Paper also finds that the Department should craft balanced policy and build coalitions on issues including cybersecurity, privacy, intellectual property, and cross-border data flows. While government has a critical role to play in ensuring that its policies enable industry to meet consumers' IoT demands, it must be sure to limit other types of regulatory intervention – and to refrain from issuing any regulations that could stifle innovation in the nascent IoT ecosystem. Prescriptive regulation, however well intentioned, could inhibit the development and deployment of such offerings. The Department, and the Administration as a whole, should ensure that government assesses any potential need for IoT regulation in a coordinated manner and, if it identifies a need for regulation is necessary, avoids creating fragmented or conflicting requirements. Policymakers at all levels of government should exercise restraint, given the complexity of the IoT and the vast potential for unintended consequences, and take only actions consistent with the core framework discussed in CTA's initial comments:[23]

- The primary goal of any IoT policy regime should be to promote innovation.
- To promote innovation, policymakers should favor market-based solutions over prescriptive regulations and apply regulation only if there is a compelling public interest in doing so (*i.e.*, in order to address demonstrable harms that cause concrete injury to consumers).[24] Such an approach is consistent with President Trump's executive actions instituting a regulatory freeze and requiring federal agencies to

[23] *See* CTA Initial Comments at 16-19.

[24] *See* Shapiro, *Want America to Innovate?*; Gary Shapiro, *HowThe Heavy Hand Of Government Stifles The On Demand Economy*, TECHDIRT (Aug. 25, 2015), https://www.techdirt.com/articles/20150824/-11370432049/how-heavy-hand-government-stifles-demand-economy.shtml.

minimize the net costs to the private sector of any new regulations.[25] CTA encourages the Department, as well as all federal agencies and the Administration, to review any new or proposed regulations with this in mind.

- 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 outcomes.

Consistent with these principles, policymakers should avoid imposing mandates that would pick technology winners or otherwise impede the growth of the IoT, such as by precluding market competition. Government also must refrain from over-reaching enforcement actions that harm consumers by increasing the cost of providing service and entering a sector without providing commensurate consumer benefit.

Cybersecurity and Privacy. The security and privacy issues 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. A lesson learned from experience with the internet economy over the past couple of decades is that consistent, effective privacy and security protections – a foundation of trust – are most likely to develop when the government itself takes a holistic view of technologies, business models, and privacy and security risks. The IoT is no different. Thus, to address privacy and security concerns, government should continue to foster global, industry-wide, consensus-driven self-regulation that is nimble and accounts for rapidly evolving technologies.[26] In the Green Paper, the Department proposes to support and

[25] *See* Exec. Order No. 13771, Reducing Regulation and Controlling Regulatory Costs, 82 Fed. Reg. 9339 (Feb. 3, 2017), https://www.gpo.gov/fdsys/pkg/FR-2017-02-03/pdf/2017-02451.pdf; Memorandum for the Heads of Executive Departments and Agencies; Regulatory Freeze Pending Review, 82 Fed. Reg. 8346 (Jan. 24, 2017), https://www.gpo.gov/fdsys/pkg/FR-2017-01-24/pdf/2017-01766.pdf.

[26] *See* CTA Initial Comments at 19.

promote policies that encourage risk-based approaches, security by design, and the ability to patch insecure software and devices; promote the use of strong encryption; and collaborate with industry on security and safety education for consumers.[27] CTA concurs.

The Green Paper recognizes that while the IoT presents some security risks to connected vehicles and consumer devices, for example, the range of IoT devices and apps precludes a single, prescriptive solution. The Department concluded that the U.S. government can play a valuable role in driving awareness and resolution of the cybersecurity issues facing IoT development. Multistakeholder efforts and industry-driven global standards organizations are very important in this regard and have a track record of success. For example, the NIST Cybersecurity Framework – developed through the public-private partnership work of multiple critical infrastructure sectors with the Department – "highlights the limitations of a 'one-size-fits-all' solution and instead is a voluntary, flexible framework that can be scaled to organizations' different needs, allowing them to take into account particular business models, assets, and other variables."[28] NTIA appropriately has used its multistakeholder processes to further catalyze industry discussion on cybersecurity-related issues, with the stated goal of achieving consensus-based positive outcomes.[29] A similar approach could address consumer safety and quality of

---

[27] Green Paper at 42-43.

[28] *Id.* at 27; *see also* CTA Initial Comments at 25; U.S. Communications Sector Coordinating Council, https://www.comms-scc.org/about-1 (last visited Mar. 10, 2017) (describing means of coordination used by the Communications Sector Coordinating Council); FCC, Advisory Committees, *Communications Security, Reliability and Interoperability Council*, http://transition.fcc.gov/pshs/-advisory/csric (last visited Mar. 10, 2017). The Communications Security, Reliability and Interoperability Council's ("CSRIC") 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. CSRIC, *Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report* (Mar. 2015), https://transition.fcc.gov/pshs/advisory-/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[29] *See, e.g.*, Stakeholder Engagement on Cybersecurity in the Digital Ecosystem, 80 Fed. Reg. 14360, 14360 (Mar. 19, 2015), https://www.gpo.gov/fdsys/pkg/FR-2015-03-19/pdf/2015-06344.pdf (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 14361 (stating that "[i]n the digital ecosystem, the rapid

service issues in the IoT by giving industry the opportunity to directly participate and shape practices that can evolve as new business and technological developments emerge. By significantly expanding the number of potential incursion points for malware, botnets and other forms of cyber threats, the IoT unquestionably presents serious security issues that must be grappled with by all elements of the marketplace, including device makers, product dealers, hardware and software vendors, service providers, and other stakeholders. The Department's experience and track record in convening multistakeholder processes will be critical to helping to forge holistic solutions to IoT security issues.

The Green Paper advocates security by design and notes that the Federal Trade Commission ("FTC") has also embraced this approach with its IoT "Start with Security" guidance.[30] CTA concurs that security must be integrated into the hardware and the software at the outset to enable robust, secure, trusted end-to-end IoT solutions. Multi-layered protection must at least protect storage, and enable device identification and authentication, software authentication, protected boot and trusted execution environment. Indeed, security should be integrated throughout the concept and design process. Attempts to bolt on security features late in the product development process are more expensive, more difficult, and prone to error. However, there is no clear consensus or straightforward path on how to implement this concept across the IoT space.

---

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., NTIA, Remarks on the Vulnerability Research Disclosure Multistakeholder Process (Sept. 29, 2015) ("[I]t 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.

[30] Green Paper at 27.

CTA also recognizes that security plays an important role in protecting consumers' privacy. Similar to other technologies, with regard to broader questions of privacy, CTA urges the Department to maintain the Green Paper's perspective of collaborating with industry experts in multistakeholder efforts and looking to existing policies and frameworks to address these questions. Although IoT devices can collect different types of personal data, or increase the amount of personal data that companies collect, a time-tested technology-neutral privacy framework based on transparency, consumer choice, security, and heightened protections for sensitive data should remain the foundation of privacy protections for the IoT, as for all other technologies. There is no need for a special or different set of privacy rules to apply to IoT devices, and such an approach would stifle – rather than advance – the evolution of the IoT marketplace.

CTA also urges the Department to recognize that a wide range of self-regulatory regimes help companies develop business practices and customer notices that effectuate their privacy obligations and safeguard consumer information privacy while fostering innovation.[31] Stakeholders already are proactively addressing IoT privacy concerns through such efforts.[32] Government action cannot match the speed and agility of these efforts, though the government – particularly the FTC – can play a helpful role in ensuring that companies keep the promises that they make to consumers about privacy protections.

Intellectual Property. The Green Paper concludes that intellectual property deserves further consideration as IoT becomes more ubiquitous.[33] It notes that patents provide incentives

[31] *See* CTA Initial Comments at 19.

[32] *See id.* at 19-20. Broadband Internet Technical Advisory Group, *Internet of Things (IoT) Security and Privacy Recommendations*, Uniform Agreement Report (Nov. 2016), https://www.bitag.org/documents-/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf.

[33] Green Paper at 33-34.

for innovators to develop better IoT devices, manufacturing practices, and infrastructure; there may be issues around standard essential patents and licensing, as well as patent quality.[34] 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."[35] 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.

Standards development. As CTA noted in its response to NTIA's initial Request for Comments, voluntary, consensus-based, global standards are best positioned to help advance IoT development and innovation because they promote interoperability and provide a clearer path along which technologies can evolve.[36] Proprietary or country-specific standards must be discouraged. CTA applauds the Green Paper's recognition of the benefits of this role for voluntary, consensus-based global standards, as well as the roles that NIST and NTIA have played in promoting the development of such standards. CTA encourages the Department to continue this work in connection with IoT-related standards, in addition to engaging with its foreign counterparts to promote voluntary standards development. Although no single forum can develop all of the standards for the IoT, maintaining a consistent approach with private sector leadership at its center provides the best chance of success in this broad endeavor. A few examples of leading global standards organizations with broad-based memberships are the Industrial Internet Consortium ("IIC"),[37] the Open Connectivity Foundation ("OCF")[38] and the

[34] *Id.* at 36.

[35] RFC at 19958.

[36] CTA Initial Comments at 8-9.

[37] *See* Industrial Internet Consortium, http://www.iiconsortium.org (last visited Mar. 10, 2017).

OpenFog Consortium ("OpenFog").[39] The IIC's more than 250 members published a security framework for the Industrial IoT last year, and the organization has 27 active test beds spanning multiple sectors around the globe and 25 more test beds in the pipeline. The OCF includes hundreds of members from diverse market sectors around the world and is developing an interoperability specification, an open source implementation, and a certification program to ensure interoperability regardless of manufacturer, form factor, operating system, service provider or physical transport technology. OpenFog has over 60 members and is growing, and has published a fog computing architecture overview in 2016 (fog computing is a type of IoT architecture), with the reference architecture framework slated for this year. CTA encourages the Department to promote the efforts of the IIC, OCF, OpenFog and other leading industry-driven, global standards organizations with large U.S. participation, such as CTA, to advance IoT innovation and development.

C. Are there specific tasks that the Department should engage in that are not covered by the approach?

The Department can work with other government entities to take additional steps toward ensuring that the U.S. IoT sector maintains its global leadership role. For example, through procurement, the government can generate demand for IoT technologies to help jumpstart the development of IoT ecosystems. In addition, changes in tax policy can help facilitate the rapid growth of the IoT sector, and 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.

---

[38] *See* Open Connectivity Foundation, https://openconnectivity.org (last visited Mar. 10, 2017).

[39] *See* OpenFog Consortium, https://www.openfogconsortium.org/about-us (last visited Mar. 10, 2017).

Another area for government action is immigration, ensuring that appropriate immigration policies are in place to grow the U.S.'s science, technology, engineering, and math ("STEM") work force to unleash the potential of the IoT sector. Strategic immigration reforms are needed to encourage U.S.-educated immigrants to remain in the U.S. to build businesses and create domestic jobs.

Finally, as discussed to some extent in the Green Paper, there is a role for government in consumer education. Building a strong partnership between the public and private sectors can help bolster the foundation for consumer confidence and trust in the IoT. As the Green Paper notes, government can play an active role in skills development to create quality career paths and can incorporate IoT into education and awareness programs.[40] At a fundamental level, the IoT depends on the collection and sharing of information among devices, and thus is premised on consumer trust and utility. In addition to the work already being done by IoT manufacturers and service providers, government can advance the interests of consumers by working with industry to develop a system of trust between users and things. Together, following the FTC's example in its *Start with Security* series, 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-protected home Wi-Fi networks with firewalls, and employing virtual private networks).

D. What should the next steps be for the Department to foster advancement of IoT?

The Green Paper proposes numerous next steps for the Department to take to help advance the IoT. Many of these proposals are consistent with CTA's perspectives on the specific subject matter areas discussed above, from global standards to spectrum to workforce

[40] Green Paper at 54.

development. These steps would meaningfully advance IoT development. Still, CTA remains concerned about the differing approaches of the many federal agencies that are active in IoT policy formulation. In order to best foster advancement of IoT in the U.S. and ensure that America leads the world, we must have a national IoT strategy that emphasizes the need to handle the IoT with a light regulatory touch and makes a commitment to coordinating federal agencies' IoT policy development activities.

As a further first step, CTA strongly encourages the Department to support the bipartisan "Developing Innovation and Growing the Internet of Things (DIGIT) Act," which would require the Secretary of Commerce to convene a working group of Federal stakeholders to provide IoT recommendations to Congress, in consultation with industry and non-governmental stakeholders.[41] While the Department's Green Paper "defer[red] to future policy makers to determine the value of crafting a national strategy[,]"[42] CTA respectfully suggests that, it is an opportune time for the Department to support the DIGIT Act as a step toward developing collaborative recommendations that can inform a national IoT strategy and, in turn, developing such strategy. A collaborative, pro-innovation IoT strategy will help solve important societal issues and drive American competitiveness for decades to come – fueling GDP, creating new jobs, and bolstering the U.S. economy.

The Department's range of expertise makes it a logical choice to play a leading role in that effort. The Department also has an overall focus on promoting innovation, economic growth, and job creation – all of which will follow from an IoT policy that avoids new prescriptive regulations and eliminates duplicative or conflicting mandates that currently exist.

[41] Developing Innovation and Growing the Internet of Things Act, S. 88, 115 Cong. (2017) ("DIGIT Act"), https://www.gpo.gov/fdsys/pkg/BILLS-115s88is/pdf/BILLS-115s88is.pdf.

[42] Green Paper at 10.

For these reasons, CTA supports having the Department take a lead role in developing an Administration policy that more comprehensively positions the United States to ensure its IoT leadership and to realize the IoT's full economic and social benefits.

III. CONCLUSION

The Department is uniquely positioned to advance policies that will help develop the IoT and advance the Administration's broader economic goals. By supporting the DIGIT Act and a national IoT strategy; making more flexible-use spectrum available; convening stakeholders to address IoT issues and incentivizing IoT solutions for next generation infrastructure; promoting voluntary, global consensus-based, industry-driven standards; supporting multistakeholder and industry efforts to drive innovation in security innovation; and harmonizing federal agency interaction – the Department has a key role to play in bringing the full benefits of the IoT to U.S. consumers, businesses, and society. In addition, the Department can promote policies that will build – and expand – a workforce that possesses the skills necessary to fully realize the IoT's potential benefits. These actions will drive United States' global leadership in the transformative IoT ecosystem. By contrast, broad, prescriptive regulatory action would derail or delay new IoT applications in the U.S., to the nation's global disadvantage. The Department should use its role in the federal government as well as its activity in international fora to promote voluntary, industry-driven global technical standards and self-regulatory approaches that promote innovation and protect consumers, rather than stifling growth with burdensome and inflexible regulations. The actions suggested in the Green Paper represent a solid step toward achieving these goals, and CTA looks forward to working with the Department and the Administration as it ensures America's IoT competitiveness and leadership into the future.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

By: */s/ Julie M. Kearney*

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

March 13, 2017