Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

In the Matter of	)	
	)	
The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things	)	Docket No. 170705023-7023-01
	)	
	)	
	)	

COMMENTS OF THE

CHAMBER TECHNOLOGY ENGAGEMENT CENTER, C_TEC

U.S. CHAMBER OF COMMERCE

Tim Day
Senior Vice President
U.S. CHAMBER OF COMMERCE
TECHNOLOGY ENGAGEMENT CENTER, C_TEC
1615 H STREET, NW
WASHINGTON, DC 20062-2000
tday@uschamber.com

Megan Brown
Umair Javed
WILEY REIN LLP
1776 K STREET, NW
WASHINGTON D.C. 20006
mbrown@wileyrein.com
Counsel to C_TEC

March 13, 2017

EXECUTIVE SUMMARY

The U.S. Chamber of Commerce Technology Engagement Center, C_TEC,[1] was established to advance technology's role in the U.S. economy. Our members are excited about the future of technology to drive growth, jobs, and life-changing advances in transportation, medicine, consumer experiences, and business operations. C_TEC promotes policies that foster innovation and creativity and sponsors research to inform policymakers and the public.

C_TEC appreciates the National Telecommunications and Information Administration's ("NTIA") efforts to help the Department of Commerce ("DOC") and the entire government to understand the role of the Internet of Things ("IoT") in the digital economy. We agree with many of NTIA's conclusions in its recently released Green Paper, particularly the recognition that new regulations are not needed; indeed, they may be counterproductive. As NTIA takes feedback on the Green Paper and considers how to support policy and innovation in the new Administration, C_TEC urges the government to think big about the future and advance IoT by:

- Promoting data–driven decisions and consistent, broad definitions that recognize the diversity of IoT;
- Promoting global, voluntary and open industry-led standards, supporting interoperability and the free flow of information;
- Promoting security through partnerships, education, and reduction of liability risk; and
- Removing barriers to infrastructure deployment and avoiding regulation and fragmentation.

NTIA can contribute to the future of IoT by coordinating government activity and insisting on data-driven decision making. As a convener of American innovators, C_TEC is ready to help the government promote the limitless potential of IoT.

[1] C_TEC is the successor to the Center for Advanced Technology and Innovation ("CATI") at the U.S. Chamber. The Chamber filed comments in response to the Notice and Request for Comments, Docket No. 160331306-6306-01.

TABLE OF CONTENTS

Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

In the Matter of	)	
	)	
The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things	)	Docket No. 170705023-7023-01

COMMENTS OF THE U.S. CHAMBER OF COMMERCE
TECHNOLOGY ENGAGEMENT CENTER

C_TEC is encouraged that NTIA's Green Paper, *Fostering the Advancement of the Internet of Things* ("Green Paper") recognizes the tremendous economic and social benefits that will derive from IoT. It rightly finds no need for IoT-specific regulation, and identifies areas where the government can promote IoT.[2] C_TEC is pleased to respond to NTIA's Request for Comments on the Green Paper because future federal IoT policy is vital to the U.S. economy. C_TEC has been engaging innovators and conducting research on IoT. We urge the government to rely on data and experience to aggressively promote IoT innovation, which has begun to take shape with innovation in verticals like autonomous vehicles and unmanned aircraft systems ("UAS"). Instead of IoT-specific laws or regulations, the government should aggressively promote infrastructure and investment, support security partnerships and innovation, and promote open, accessible global markets for IoT services and products.

I. CONGRESS SHOULD PASS THE DIGIT ACT AND PROMOTE IOT POLICY BASED ON DATA, LIKE THAT DEVELOPED BY C_TEC.

Congress has taken a prudent approach, looking to promote innovation and do no harm. This is manifest in the bipartisan DIGIT Act, which C_TEC strongly supports. Adoption of the

[2] Dep't of Commerce, Internet Policy Task Force & Digital Economy Leadership Team, Green Paper, *Fostering the Advancement of the Internet of Things* (Jan. 2017) ("Green Paper").

DIGIT Act would be a critical first step in the public-private development of a national IoT strategy based on data and real world experience. The DIGIT Act will bring together stakeholders in government and industry to shape policy, ensuring that the United States realizes the full economic potential of IoT and remains a leader in this next chapter of the Internet.[3] The DOC should support the DIGIT Act, which will encourage collaboration and build on momentum already established by NTIA on these issues.

Likewise, C_TEC lauds the formation of the Congressional Caucus on the Internet of Things and the bipartisan Internet of Things Working Group. The Caucus is developing a foundation for thoughtful public policy on IoT, and the Working Group has met with experts, stakeholders, and leaders in a number of industries to discuss the benefits and challenges of IoT and the role of the government.[4] These efforts represent the right approach for IoT, and they will form the foundation for data-driven and consistent policy.

As IoT matures, policymakers must seek out meaningful data on markets, uses, innovation, and consumer expectations, in order to make informed judgments. Imposing rules without evidence of problems can have the unintended consequence of limiting innovation and raising costs. Measuring the benefits of IoT innovation will be challenging, but policymakers should insist on data about IoT uses and consumer behavior. C_TEC has been generating meaningful data to inform policy discussions. Its website, http://ctecintelligence.com/, has a trove of data about consumer understandings and expectations on everything from the future of

---

[3] *See* U.S. Chamber of Commerce, "U.S. Chamber's CATI Commends Internet of Things Working Group, Highlights Economic Benefits of Innovative Technology" (Mar. 1, 2016), available at https://www.uschamber.com/press-release/us-chamber-s-cati-commends-internet-things-working-group-highlights-economic-benefits.

[4] Internet of Things Working Group, Year-End White Paper (December 30, 2016), available at http://latta.house.gov/uploadedfiles/iot_working_group_white_paper.pdf.

IoT to the causes of the October 2016 DDoS attack. C_TEC looks forward to sharing its expertise with policymakers as the IoT matures.

II. BROAD, FLEXIBLE DEFINITIONS SHOULD REFLECT IOT'S EVOLUTION AND COMPLEXITY.

Scoping and definitional issues are critical to discussing IoT. The Green Paper notes several definitions, but finds no consensus on a definition or the need for one.[5] The IoT ecosystem is incredibly diverse in potential use cases, users, and contexts. While this diversity is a virtue, it can make policy discussions diffuse and over-inclusive. Some IoT reports cover too much ground, failing to differentiate "managed IoT" from consumer-controlled IoT; likewise, industrial uses will be governed far differently than individual consumer uses. And government procurement and management of IoT services will raise different issues than private deployments. The issues in various IoT settings will differ, so rigor should be used to clarify discussions. C_TEC supports a broad definition that illustrates the diversity of IoT deployments and use cases and remains flexible so that is not instantly obsolete or inherently under- or over-inclusive.

In C_TEC's view, the IoT is made up of "things" that are securely connected through a network—often to the cloud—from which data can be shared and analyzed to create value. But it is not just the "things"—in fact, focusing on devices ignores the broader, complex IoT ecosystem. The IoT also connects "things" like appliances, machinery and cars to the Internet, shares and analyzes the data generated by these things, and extracts meaningful insights that can create new opportunities and solve societal problems.

C_TEC views the IoT as made up of two major segments: Consumer IoT and Industrial IoT. The Consumer IoT connects devices like smart TVs, household appliances, gaming

[5] Green Paper at 5 (quoting several comments and approaches).

consoles, wearables and smartphones. The Industrial IoT provides connectivity in industrial environments, using devices like factory equipment, retail systems, security cameras, medical devices and digital signs. While there may be overlap—some devices or services may be used in both settings—recognizing these two broad categories can focus policy discussions.

Likewise, as it develops, IoT may evolve into "managed" and "non-managed" products and services. Managed IoT may be made up of value-add services and products integrated into broader offerings, IoT services and devices that are managed by a third party provider, or cloud-based IoT management platforms. Microsoft's Azure IoT Suite, Cisco's Jasper, Intel's IoT Platform, and Amazon Web Services are just a few examples of available, managed IoT platforms. Managed service providers are exploring markets, which may include cloud security, network, data, and device management. Non-managed IoT could include individual devices purchased from third parties for end users to connect and manage. User needs, as well as expected network, service, and device capabilities, may differ across these settings, but these markets must develop before policymakers can begin to assess needs or gaps.

The government should promote accuracy and flexibility in discussing IoT by making clear to all stakeholders that the ecosystem is complex and evolving and is likely to encompass different user types and vastly different distribution and service models. All parts of the ecosystem—software developers, manufacturers, service providers, cloud operators and network owners—will have to innovate and collaborate to drive IoT into the future.

III. A NATIONAL STRATEGY SHOULD PROMOTE VOLUNTARY, OPEN, AND CONSENSUS-BASED STANDARDS THAT FACILITATE INTEROPERABILITY AND OPEN MARKETS.

The full benefits of IoT will be achieved only if technologies operate in an open and interoperable global environment. The Green Paper recognizes that a private-sector led approach to standards development, with appropriate government participation, is fundamental. This is the

only way to develop voluntary, consensus-based, and global standards that will promote open markets and economies of scale.[6] Industry is leading the development of technological standards, promoting interoperability, and urging free and open cross-border data flows. The U.S. government should actively support these efforts, whether or not policy-makers call their effort a "national strategy."

A. Industry is Active in Global Efforts to Address IoT.

Multiple global industry efforts are underway, setting standards, testing solutions, and building platforms for IoT services, devices and networks. A few examples include:

- The Industrial Internet Consortium. The IIC is a global, member supported organization that promotes the accelerated growth of the Industrial IoT by coordinating ecosystem initiatives to securely connect, control and integrate assets and systems of assets with people, processes and data using common architectures, interoperability and open standards to deliver transformational business and societal outcomes across industries and public infrastructure. It has over 250 members and 27 active testbeds all over the world from more than a dozen different segments, with another 25 in the pipeline. Its Security Framework was published in September of 2016.

- The Open Connectivity Foundation. OCF is defining connectivity requirements to improve interoperability between the billions of devices making up the IoT. OCF will deliver a specification, an open source implementation and a certification program ensuring interoperability regardless of manufacturer, form factor, operating system, service provider or physical transport technology. OCF has hundreds of members across North America, Asia, Europe and other geographies, from diverse markets including: Automotive, Consumer Electronics, Enterprise, Healthcare, Home Automation, Industrial and Wearables, among others.

- Open Fog Consortium. OFC is driving industry and academic leadership in fog computing architecture, testbed development, and a variety of interoperability and composability deliverables that leverage cloud and edge architectures to enable end-to-end IoT scenarios. It has over 60 members and published its OpenFog architecture overview in 2016, with the reference architecture framework to be released in 2017.

Government should support these kinds of voluntary, open participation, and consensus-based efforts. Such efforts should inform federal policy and help federal evaluation of

[6] Green Paper at 44.

technology and standards, such as work at the National Institute of Standards and Technology ("NIST") on aspects of IoT and connectivity. As the Green Paper recognizes, governments also can work as both facilitators and conveners of industry-led efforts, ensuring full industry participation.[7] Government experts may even participate in these industry-led efforts as needed.

B. Interoperability Will be Important to Global IoT.

Industry can and should lead the development and adoption of technical and interoperability standards for networks, systems, services and devices that will make up the IoT. However, the Green Paper rightly recognizes that national governments have an important coordinating role to play. As countries and intergovernmental organizations advance their own national strategies and standards for IoT, the U.S. government should continue to promote interoperable solutions and multistakeholder approaches to address policy and technical challenges. A fragmented ecosystem with non-interoperable technologies will only serve to undermine IoT deployment and consumer adoption.

Not surprisingly, many nations recognize IoT as a high priority. While some are developing strategies to support interoperable deployments, others are focused on IoT as a target for protectionist regulation. The latter is being expressed in many ways, including a preference for proprietary and non-technologically neutral technical standards; an increased focus on privacy, security (cyber and national), and domestic consumer protection regulation; protection of domestic industries and national champions; and an increased role of national governments and intergovernmental organizations in unregulated or loosely regulated markets.

Intergovernmental organizations, in particular, are seeking influence. They are considering IoT-specific work items that threaten to diminish the IoT marketplace. For example,

---

[7] Green Paper at 44.

the United Nation's International Telecommunication Union ("ITU") is considering proposals for work on technical, economic, and policy aspects of identification and authentication standards for IoT, permanent roaming, and top-down interoperability standards. ITU outputs often form the basis for domestic regulation. Thus, whether NTIA or the DOC calls the U.S. effort a "national strategy," the United States' international engagement will be key to a globally connected IoT in which U.S. innovators play a leading role.

C. The U.S. Must Work to Facilitate Cross-Border Data Flows.

A major threat to global IoT is forced data localization and arbitrary barriers to the flow of information that will be the lifeblood of the IoT. Many countries have adopted or are considering data localization requirements. These measures take a variety of forms: data storage requirements; local goods/services content requirements; customs requirements; government investment/tax requirements; and encryption requirements, among others. Such rules can be counterproductive and constrain the ability of U.S. companies to provide services globally.

The U.S. government should guard against these efforts and pursue IoT strategies that may receive international acceptance. In addition, the government should work with other countries and stakeholders to advance globally harmonized IoT policies. Such policies should champion the seamless flow of information across borders and procurement policies that encourage government adoption of IoT technologies. In the short to medium term, the U.S. government can use existing bilateral and multilateral dialogues to advance these policies, including at the G-20, ITU, and the Organisation for Economic Co-operation and Development.

IV. SECURITY IS BEST ADVANCED THROUGH COLLABORATION, CONSUMER EDUCATION, AND REDUCING LIABILITY CONCERNS.

The Green Paper is correct that IoT security challenges should be met with flexible risk-based solutions and that there "is no single prescription or set of best practices" for security.[8] The Green Paper addressed security by design, patching, device capabilities, and data collection. Each of these complex areas will benefit from ongoing work, but if the government wants to unleash real change, it must be creative in removing barriers and aligning incentives. C_TEC suggests the government take three steps to promote IoT security: support more robust, protected collaboration; promote consumer awareness and responsibility; and address liability concerns.

First, the government should continue to promote private collaboration to share information and develop best practices, as the Green Paper recommended. When it comes to security, government should not presume to have solutions, whether it relates to a kind of two-factor authentication, a cadence or approach to device patching, network design, consumer disclosures, or other solutions. Companies invest substantial amounts on security by design, monitoring, mitigation, and next-generation security. They work in domestic and international bodies to develop standards for the networks that will support IoT. They share information in formal and informal settings. And, they respond daily to attacks from nation-states, hacktivists, and criminals, taking measures to mitigate emerging threats like ransomware and DDoS attacks.

Industry collaborates well with government. The Department of Homeland Security ("DHS") leads numerous partnerships. At the Federal Communications Commission ("FCC"), the Communications Security Reliability and Interoperability Council ("CSRIC") IV worked to map the NIST Cybersecurity Framework to the communications sector, and CSRIC V is actively looking at network cybersecurity. Likewise, NTIA is looking at IoT security and vulnerability

[8] Green Paper at 24.

disclosures, in ongoing multistakeholder efforts.[9] NIST is actively engaged as well; the NIST Cybersecurity Framework is a prime example of effective public-private collaboration. To really foster information-sharing, the government has to seriously consider how to protect information shared, and how to limit public disclosures about security issues. Companies will be more likely to collaborate when they do not fear disclosure, regulation, oversight, or public disdain over their practices and vulnerabilities.

Second, the government can encourage better consumer awareness, which will be critical to the success of IoT. NTIA recognized this, but its proposed next steps do not go far enough.[10] Consumers will play a vital role in securing the IoT ecosystem, by managing their devices, using passwords and other tools, accepting available upgrades, paying attention to connection security, and other basic cyber hygiene. But some consumers do not appreciate the need to take responsibility for their connected activity. One recent survey looked at suboptimal consumer security choices. Researchers found that "respondents most often rejected security behaviors because they were inconvenient."[11] Specifically, "inconvenience … was the most common reason (50%) selected … for why they did not complete software updates."[12] Respondents also resisted anti-virus software and two-factor authentication: "45% [of respondents] used 2FA on some, but not all services; and 28% never used 2FA;" the report found "[i]nconvenience was also the most common reason given by respondents for not using 2FA (41%)."[13]

---

9 Green Paper at 41.

10 Green Paper at 43.

11 Elissa M. Redmiles, Sean Krossy, and Michelle L. Mazurek, University of Maryland, *Johns Hopkins University, How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior*, CCS'16, October 24 - 28, 2016, Vienna, Austria.

12 *Id.*

13 *Id.*

Industry has been working hard to promote awareness and is encouraged that more consumers are using passwords and PINs.[14] Government promotes education,[15] and third party resources abound.[16] C_TEC has been pioneering research into consumer attitudes toward IoT, because working from assumptions, anecdote, or fear may lead to policies that discourage innovation. For example, some policymakers were concerned after the October DDoS attack involving an IoT botnet. Events like this can take on outsized importance, and it is important that security issues be accurately addressed so that we do not scare consumers or policymakers away from new technology. Indeed, consumers are becoming more attuned to security and technology issues; a poll commissioned by C_TEC shows that, despite the DDoS attack, a majority still see the benefits of IoT devices to their lives and the economy.[17] NTIA and the DOC may want to coordinate national awareness efforts, perhaps with other agencies or third parties, to elevate public appreciation of the importance of security and overcome any inertia or confusion that may limit use of resources.

---

[14] *See, e.g.*, Majority of Americans Use PINs or Passwords to Protect their Mobile Devices and Personal Information, CTIA-The Wireless Association (2015) http://www.ctia.org/industry-data/press-releases-details/press-releases/majority-of-americans-use-pins-or-passwords-to-protect-their-mobile-devices-and-personal-information

[15] *See* US-CERT, Tips, available at https://www.us-cert.gov/ncas/tips; US-CERT, Home and Business, available at https://www.us-cert.gov/home-and-business; Federal Trade Commission, FTC and NCUA Offer Cyber Security Tips (Oct. 20, 2015) available at https://www.consumer.ftc.gov/blog/ftc-ncua-offer-cyber-security-tips.

[16] *See* Consumer Reports, Guide to Internet Security, available at http://www.consumerreports.org/cro/electronics-computers/guide-to-internet-security/index.htm; National Cyber Security Alliance, StaySafeOnline.org, available at https://staysafeonline.org/; Lookout, Security for the Mobile Generation, available at https://www.lookout.com/ (describing some tools available to secure mobile devices).

[17] Sean Hackbarth, U.S. Chamber of Commerce, "Americans Aren't Freaking Out Over the Internet of Things DDOS Attack" (Oct. 31, 2016), available at https://www.uschamber.com/above-the-fold/americans-arent-freaking-out-over-the-internet-things-ddos-attack.

Finally, policymakers should seriously consider private sector concern about the risks and uncertainty associated with security efforts like sharing information, making public assurances, and disclosing vulnerabilities. IoT innovators, network operators, and service providers are rightly concerned about unintended consequences. Indeed, the White House *Commission on Enhancing National Cybersecurity* noted the possibility that liability fears could stymie IoT innovation and recommended that several agencies assess the state of the law.[18] These fears are credible, and based on real world experience. Security claims have been exploited by opportunists to harm U.S. companies making investments in U.S. IoT.[19] They can lead to non-meritorious lawsuits; for example, vulnerability disclosures have led to burdensome class-actions, even where no exploitation or breach occurred.[20] Security issues can also be the basis for claims—some meritorious, some not—of deception or unreasonableness of security practices.[21] Network defense and information sharing also carry risk. Some mitigation measures may put network operators and others at risk under federal privacy laws[22] if, for

---

[18] Commission on Enhancing National Cybersecurity, Report on Securing and Growing the Digital Economy, Action item 2.1.3, (December 1, 2016), available at https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf ("*Commission on Enhancing National Cybersecurity*").

[19] *See* M. Goldstein, N.Y. Times, "Hedge Fund and Cybersecurity Firm Team Up to Short-Sell Device Maker" (Sept. 8, 2016) available at https://www.nytimes.com/2016/09/09/business/dealbook/hedge-fund-and-cybersecurity-firm-team-up-to-short-sell-device-maker.html?_r=0.

[20] *See, e.g.*, *Flynn v. FCA US LLC*, 2016 WL 5341749 (S.D.Ill. 2016) (granting in part and denying in part defendants' motions to dismiss in case alleging consumer harm from vulnerability); *Cahen v. Toyota Motor Corp*. 147 F.Supp.3d 955 (2015), *appeal pending* (9th Cir. 2017) (District Court dismissed for lack of standing a class action in which plaintiffs allege that Toyota and GM violated California law by selling cars allegedly susceptible to hacking).

[21] *See, e.g.*, Release, "FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras" (January 2017), available at https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate.

[22] *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a).

example, they fall outside of the Cybersecurity Information Sharing Act's ("CISA")'s authorization of defensive measures.[23] Likewise, protected sharing is focused on cyber threat information, not on product development issues or general vulnerabilities.

Policymakers should encourage innovation, appropriate information sharing, and other security-enhancing steps while providing reliable protections for proprietary data and sensitive business information. In IoT, complex new services and products evolve, are customizable, and interact with or depend on hardware, software, network operators, application developers, and others in a complex ecosystem. Further complicating things, they are under constant siege by good guys and bad guys. To assure innovators they will not be punished for doing the right thing, additional incentives and protections from liability should be explored.[24] C_TEC is convening groups to discuss these concerns, and looks forward to working with NTIA and others to solve these important questions.

V. INFRASTRUCTURE DEPLOYMENT AND UNIFORM REGULATORY ENVIROMENTS WILL BE CRITICAL, AS DEMONSTRATED IN MATURING IOT VERTICALS LIKE UAS AND AUTONOMOUS VEHICLES.

Meeting IoT demands will require investment in the modernization of telecommunications infrastructure and build-out of additional broadband capable networks. This deployment can be stymied by state and local barriers and regulatory fragmentation. C_TEC

---

[23] *See Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures*, June 15, 2016, available at https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf.

[24] IoT has the potential to be as disruptive and beneficial as the Internet itself. The number of devices and services built for IoT has risen sharply in recent years; connectivity is improving productivity in the private sector, building more resilient and energy-efficient cities, improving the delivery and management of healthcare, and creating safer and more accessible homes. IoT also can help government provide essential services. IoT is a boundless platform for innovation, and there is no way to predict all of the opportunities it will create. *See, e.g., Commission on Enhancing National Cybersecurity*.

urges NTIA and the DOC to tackle each potential source of delay, on their own and with other agencies.

First, IoT needs infrastructure deployment to proceed rapidly, without undue barriers. The expected increase in device connectivity associated with IoT will "dramatically increase demands upon the nation's information and communications infrastructure" and "could put stress on legacy networks as well as more recently deployed all-Internet Protocol systems."[25] To ensure that the infrastructure to support IoT continues to expand, the Green Paper proposes to coordinate with the private sector and with federal, state, and local government partners to promote access to infrastructure.[26] Even so, the costs and delays resulting from a web of federal, state, and local review requirements threaten to slow deployment and shift resources away from infrastructure investment and innovation.

Notwithstanding the shrinking size of communications facilities like "small cells," and the burgeoning demand for the data they will transmit,[27] the regime for siting is outdated and cumbersome. Some localities remain focused on slowing deployments and challenging efforts by Congress and the FCC to smooth the way. There also are federal obstacles, such as burdensome environmental, cultural, and historic review processes that have become outdated. C_TEC supports the Green Paper's proposal to coordinate with the private sector and federal, state, and local partners to encourage infrastructure deployment and investment, but the government should do more. C_TEC applauds the FCC's continued focus on streamlining

---

25 Green Paper at 16.

26 Green Paper at 23.

27 "Small cells range in size, with some as small as a slightly thicker iPad, going up to the size of a large hiker's backpack." Cheng, CNET, "The carriers' not-so-secret weapon to improve cell service" (June 9, 2013), available at https://www.cnet.com/news/thecarriers-not-so-secret-weapon-to-improve-cell-service/.

deployment of small cell infrastructure through improved siting policies[28] and urges NTIA to support those efforts. On a broader scale, as the Administration and Congress contemplate infrastructure investment, they should prioritize opportunities to integrate future-looking IoT solutions, enabling the U.S. to lead the world.

Second, regulatory uncertainty and fragmentation are barriers to innovation, as C_TEC knows firsthand. Autonomous vehicles and UAS are two relatively advanced examples of IoT, and they show how varied regulatory regimes can burden innovation. The automobile industry, for example, is on the cusp of a technological transformation that may catalyze an unprecedented advance in safety on U.S. roadways. Autonomous vehicles are being tested in select cities and are poised to improve the driving experience by improving safety, reducing traffic congestion, and enhancing mobility of many segments of the population, including the elderly and disabled.[29] However, automakers face a patchwork of state laws and regulations which could reduce investment and public confidence in technologies like autonomous vehicles.[30] Likewise, UAS are on the verge of commercial deployment and will be used to save lives, improve health and safety, drive economic growth, and reduce costs for businesses and consumers. The Federal Aviation Administration ("FAA") continues to consider rules that would allow small UAS to fly over people. Private effort is driving discussions of privacy and safety in UAS; for example,

---

[28] *See* Public Notice, *Streamlining Deployment of Small Cell Infrastructure By Improving Wireless Facilities Siting Policies*, DA 16-1427, 1 (FCC 2016).

[29] The U.S. Department of Transportation recently designated 10 "proving grounds" to encourage safe testing of automated vehicle technologies. *See* Insurance Journal, "10 U.S.-Designated Autonomous Vehicle Testing Sites," available at http://www.insurancejournal.com/news/national/2017/02/21/442453.htm.

[30] Indeed, the U.S. Department of Transportation's Federal Automated Vehicles Policy recognizes that a patchwork of inconsistent laws and regulations among the 50 states could delay the widespread deployment of these potentially lifesaving technologies. U.S. Department of Transportation, National Highway Traffic Safety Administration, *Federal Automated Vehicles Policy* (September 2016).

C_TEC organized a working group on advancing policies that ensure UAS are used safely and without compromising individual privacy.[31] But like autonomous vehicles, UAS are subject to a patchwork of state laws regarding privacy. These and other IoT technologies need a uniform, reliable regulatory environment.

C_TEC has been exploring the effects of state and local policy on emerging technologies and promoting federal efforts to ensure that companies are not faced with a patchwork of laws and regulations.[32] This experience can help shape federal policy. Much like earlier phases of the Internet, IoT will flourish, and the U.S. will effectively compete on the world stage, under a light-touch, market-driven approach guided by technological advancements, not regulatory classifications or silos. Regulation can have unintended consequences, by dictating specifications, approaches or business models that become obsolete—or worse, create vulnerabilities. NTIA and the DOC should encourage regulators to coordinate their interest in IoT, and avoid duplicative and overlapping activities.

VI. CONCLUSION.

C_TEC is enthusiastic about the potential for IoT to improve the United States' economy and society. The Green Paper generally takes the right approach, but NTIA can take more aggressive and creative action to spur IoT. C_TEC urges NTIA and the DOC to look at how they and others in the federal government can aggressively champion investment and deployment of IoT. This includes supporting fast passage of the DIGIT Act, promoting

---

31 Tim Day, U.S. Chamber of Commerce, "Innovation – It's Social, Local and Global and the Chamber's C_TEC is Helping Lead the Way" (Sep. 20, 2016) available at https://www.uschamber.com/above-the-fold/innovation-it-s-social-local-and-global-and-the-chamber-s-ctec-helping-lead-the-way.

32 *Id.*

consumer awareness, leading internationally, and removing barriers to investment and innovation.

C_TEC looks forward to partnering with policymakers to enable U.S. innovators to build and deploy IoT services that will boost the American economy and society.

Respectfully submitted,

/s/ Tim Day
Tim Day
Senior Vice President
U.S. CHAMBER OF COMMERCE
TECHNOLOGY ENGAGEMENT CENTER, C_TEC
1615 H STREET, NW
WASHINGTON, DC 20062-2000
tday@uschamber.com

Megan Brown
Umair Javed
WILEY REIN LLP
1776 K Street, NW
Washington D.C. 20006
mbrown@wileyrein.com
Counsel to C_TEC

March 13, 2017