
# FOSTERING THE ADVANCEMENT OF THE INTERNET OF THINGS

THE DEPARTMENT OF COMMERCE
INTERNET POLICY TASK FORCE &
DIGITAL ECONOMY LEADERSHIP TEAM

January 2017

# TABLE OF CONTENTS

## 1. Executive Summary

The Internet of Things (IoT) – in which connected devices are proliferating at an unprecedented rate – is a technological development that is transforming the way we live and do business. IoT continues the decades-long trend of increasing connectivity among devices and the Internet, bringing online everything from refrigerators to automobiles to factory inventory systems. At the same time, IoT encompasses a widening scope of industries and activities and a vastly increasing scale and number of devices being connected, thus raising the stakes and impacts of broad connectivity.

The prospective benefits of IoT to personal convenience, public safety, efficiency, and the environment are clear. IoT has the potential to make our highways safer by enabling connected vehicles to interact with each other to prevent accidents, to make quality health care more accessible through remote monitoring devices and telehealth practices for those who cannot easily travel, and to reduce waste and improve efficiency both in factory supply chains and in the running of cities. It even has the potential to create new industries and consumer goods that have yet to be imagined. For the full potential to be realized, however, the necessary infrastructure and policies must be in place, including strategies to respond to the challenges raised in areas such as cybersecurity and privacy.

Due to its expertise in the issues raised by IoT, as well as its economy-wide perspective, the Department of Commerce (Department) is well placed to meet these challenges and to champion the development of a robust IoT environment that benefits consumers, the economy, and society as a whole.

With an April 2016 Request for Comment, "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things,"[1] the Department of Commerce sought to review the current technological and policy landscape relating to IoT**.** A broad array of stakeholders – from the private sector, academia, government, and civil society – offered perspectives[2] in response to the request. In September 2016, the Department hosted a workshop[3] to delve deeper into the questions raised by the Request for Comment, and to explore some of the related issues arising from the public comments.

This paper represents the Department's analysis of those comments. It also identifies key issues that can impact the deployment of IoT technologies, highlights potential benefits and challenges, and discusses what role, if any, the U.S. Government, particularly the Department of Commerce, should play in this evolving landscape.

---

[1] *See* https://www.federalregister.gov/d/2016-07892

[2] *See* https://ntia.doc.gov/federal-register-notice/2016/comments-potential-roles-government-fostering-advancement-internet-of-things

[3] *See* https://ntia.doc.gov/other-publication/2016/09012016-fostering-advancement-internet-things-workshop-webcast

Over the past few decades in the United States, the role of government largely has been to establish and support an environment that allows technology to grow and thrive. Encouraging private sector leadership in technology and standards development, and using a multistakeholder approach to policy making, have been integral elements of the government's approach to technology development and growth. Following a review of public comments, meetings with stakeholders, and the public workshop, it is clear that while specific policies may need to be developed for certain vertical segments of IoT, the challenges and opportunities presented by IoT require a reaffirmation rather than a reevaluation of this well-established U.S. Government policy approach to emerging technologies.

The goal of this paper is to identify elements of an approach for the Department of Commerce to foster the advancement of the Internet of Things. The record of comments underlying this green paper, however, does set forth a series of issues that should be considered in any future discussions related to the possibility of a national IoT strategy. The Department heard a strong message from the submitted comments that coordination among U.S. Government partners would be helpful, because of the complex, interdisciplinary, cross-sector nature of IoT. A federal coordination structure for these issues may also be helpful when working with international and private sector partners.

This paper begins with an overview of IoT, including definitional issues, the benefits of IoT, the possible role of government in fostering the IoT environment, and some of the international considerations that, due to the global nature of the Internet and connected technologies, are inherent in the issues discussed in the rest of the paper. The next section lays out an approach for Departmental action organized around four engagement areas. The section thereafter provides a review and analysis of the comments, current Department initiatives, and next steps for each engagement area. Consistent with the established U.S. Government policy approach to emerging technology, this approach proposes the following principles:

---

- The Department will lead efforts to ensure the IoT environment **is inclusive and widely accessible** to consumers, workers, and businesses;
- The Department will recommend policy and take action to support a **stable, secure, and trustworthy** IoT environment;
- The Department will advocate for and defend a **globally connected, open, and interoperable** IoT environment built upon industry-driven, consensus-based standards; and
- The Department will encourage IoT **growth and innovation** by encouraging expanding markets and reducing barriers to entry, and by convening stakeholders to address public policy challenges.

---

The approach identifies four broad areas of engagement to advance these principles:

- **Enabling Infrastructure Availability and Access:** Fostering the physical and spectrum-related assets needed to support IoT growth and advancement.
- **Crafting Balanced Policy and Building Coalitions:** Removing barriers and encouraging coordination and collaboration; influencing, analyzing, devising, and promoting norms and practices that will protect IoT users while encouraging growth, advancement, and applicability of IoT technologies.
- **Promoting Standards and Technology Advancement:** Ensuring that the necessary technical standards are developed and in place to support global IoT interoperability and that the technical applications and devices to support IoT continue to advance.
- **Encouraging Markets:** Promoting the advancement of IoT through Department usage, application, iterative enhancement, and novel usage of the technologies; and translating the economic benefits and opportunities of IoT to foreign partners.

The approach proposes engagement on a set of cross-cutting issues across these contexts from cybersecurity and privacy to innovation and intellectual property, with all stakeholders at the local, tribal, state, federal, and international levels. The green paper delves in depth into each of these areas of engagement, summarizing commenter feedback, describing current DOC initiatives, and proposing next steps (summarized in Appendix A: Proposed Next Steps).

The publication of this green paper will be followed by a further Request for Comment that will solicit feedback on the findings of the paper and the proposed approach and next steps. This further consultation will inform the Department's approach and next steps as we work with interagency partners on the U.S. Government's approach to IoT.

## 2. The Internet of Things (IoT) Landscape

### A. Unique Opportunities and Challenges

The Request for Comment's initial question – and likely the most important one – was whether IoT is different from technological issues that we as a society have already faced, or at least different enough to merit specific attention and/or different policy responses. Based on the collective comments, the responses at the workshop, and our conversations with stakeholders we have concluded that IoT *is* different in important aspects:

1) **Scope**: IoT is connecting a wider range of systems and devices than ever before, enabling greater integration of previously distinct industries, sectors, and activities. This will require new forms of cross-sector and cross-government collaboration, knowledge sharing, and alignment. From wearable devices that track infant heartbeats to supply chains that are capable of tracking an individual soda can from production to recycling, from connected vehicles to self-monitoring bridges, IoT portends significant and in some

cases revolutionary changes. IoT applications offer the potential for industry, government, and individuals to reap benefits in terms of increased efficiency, safety, and convenience that were previously impossible. At the same time, these industries and government agencies – and society as a whole – will need to grapple with issues that are inherent to connectivity: cybersecurity, access, data flows, education, workforce and labor impacts, cultural and socio-political differences, intellectual property rights, and privacy.

2) **Scale**: The number of connected devices coming online is growing rapidly. Cisco estimates that, between the years of 2015 and 2020, the number of connected devices in the United States will nearly double from 2.3 billion to 4.1 billion; globally connected devices will increase from 16 billion to 26 billion over the same period.[4] McKinsey Global Institute has projected that, by 2025, the overall impact of these devices on the global economy will be between $4 trillion and $11 trillion.[5] This rapidly changing environment will have broad implications. As described by commenters, the sheer magnitude of IoT devices connected will impose significant challenges for the current infrastructure, including stability, capacity, resilience, policy and regulatory consistency, and international cooperation.
3) **Stakes**: While many commenters argued that IoT is an evolution rather than a revolution in information and communications technologies,[6] the increased scale and scope produces a qualitative change in the stakes involved in connectivity. 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.[7] This represents a shift in the potential physical effects of incidents which, in the past, were generally isolated to industrial control system environments. Similarly, it is more important than at any time in the past to ensure that current and future policies foster an innovative and adaptive environment to realize the full potential of technology. As one commenter noted, the importance of well-crafted policy to address potential

[4] Cisco, VNI Complete Forecast Highlights Tool (2016), http://www.cisco.com/c/m/en_us/solutions/service-provider/vni-forecast-highlights.html ("Global" and "United States" selected).
[5] McKinsey Global Institute, Unlocking the Potential of the Internet of Things (June 2015), http://www.mckinsey.com/business-functions/business-technology/our-insights/the-Internet-of-things-the-value-of-digitizing-the-physical-world.
[6] *See, e.g.* Ligado Networks Comment at 8; 5G Americas Comment at 3; Cisco Systems Comment at 2. See also, comments of John Godfrey, Samsung, Fostering the Advancement of the Internet of Things Workshop, September 1, 2016, Transcript, 81, https://www.ntia.doc.gov/files/ntia/publications/09012016-iot-workshop.pdf. For a thorough discussion of this argument, *see* Steve Case, The Third Wave, Simon and Schuster (April 2016).
[7] The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things NOI, 81 Fed. Reg. at 19956-02. For views of respondents on this point, see Future of Privacy Forum Comment at 5.

> barriers to adoption, innovation, and trust will only increase as more devices gain connectivity.[8]

The Department believes that IoT poses qualitatively different opportunities and challenges from those that society has dealt with before. This is because the existing opportunities and challenges of the Internet are emerging in new contexts, with greater reach and impact. These characteristics of IoT support a strong case for the U.S. Government both to pursue policies that foster IoT innovation and growth, and to promote consumer trust and safety. At the same time, it is also important to recognize the policies and practices the U.S. Government has followed for decades to create environments in which emerging technologies have thrived, and to acknowledge that those policies and practices form a strong and essential foundation for developing approaches that advance IoT applications.

## B. Describing IoT

There was no consensus among commenters on a formal definition of IoT, or even on whether a common definition would be useful.[9] Definitions vary across industry and across parts of government; the Department agrees with the commenters that emphasized the need to allow the IoT environment to grow without the restrictions of labels or specific definitions that could inadvertently limit the applications, innovations, and overall potential of IoT.[10] Microsoft asserts that:

> IoT is surrounded by definitional challenges. There is no universally agreed-on definition of IoT, just as there is not universal agreement that the phenomenon itself is named IoT. Rather than defining IoT narrowly, in a manner that may limit the scope of its potential applications, we urge NTIA to consider recognizing that the term IoT does not simply describe a new type of technical architecture, but a new concept that defines how we interact with the physical world.[11]

[8] Samsung Comment (June 2, 2016) at 1.
[9] There is lack of consensus among stakeholders between the terms "cyber-physical systems" (CPS) and IoT. In a NIST-coordinated effort, stakeholders have chosen to define cyber-physical systems as "smart systems that include engineered interacting networks of physical and computational components," and noted that "[t]here is significant overlap between these concepts, in particular CPS and IoT, such that CPS and IoT are sometimes used interchangeably; therefore, the approach described in this CPS Framework should be considered to be equally applicable to IoT" (https://pages.nist.gov/cpspwg/). A NIST publication also describes a concept labeled "Network of Things," which can include IoT and is composed of sensors, aggregators, communication channels, an eUtility, and a decision trigger (NIST 800-183; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf).
[10] *See, e.g.*, State of Illinois Comment at 8-9; Trans-Atlantic Business Council Comment at 2; United States Council for International Businesses Comment at 2, 7; Verizon Comment at 4-5; Association for Computing Machinery U.S. Public Policy Council Comment at 3.
[11] Microsoft Comment at 3.

The U.S. Council for International Business suggested that "a precise, exclusive definition of the IoT is not necessary at this point,"[12] and the Trans-Atlantic Business Council advocated that "[a]ny definition should be flexible enough to adapt as IoT further develops."[13]

Many commenters suggested a definition based on particular attributes of devices, activities, or the integration of sensors, actuators, and/or network connectivity.[14] IBM referred to IoT "as the growing range of Internet-connected devices that capture or generate an enormous amount of data every day along with the applications and services used to interpret, analyze, predict and take actions based on the information received."[15] The Center for Data Innovation commented that IoT is device-based, with the "term used to describe the set of physical objects embedded with sensors or actuators and connected to a network."[16] Vodafone commented that it does not focus on the devices, but rather describes IoT as a "dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols" that connects to smart 'things.' "[17]

Other commenters did not focus on connectivity in their proposed definitions. The American Bar Association Section of Science & Technology Law argued that "IoT is not itself a 'thing,' device or product," but rather "it is a conceptual structure consisting of tangible things (e.g., commercial and consumer goods containing sensors), real estate and fixtures (e.g., roads and buildings containing sensors), plus intangibles (e.g., software and data), plus a range of services (e.g., transmission, development, access contracts, etc.)."[18] The Center for the Development and Application of Internet of Things Technologies at Georgia Tech stated that "of all the many facets of the Internet of Things as it is understood today, the one single groundbreaking element is not the connectivity … [but] the smartness of things."[19] The President's National Security Telecommunications Advisory Committee, in its 2014 Report to the President on the Internet of Things, described IoT as "a decentralized network of objects, applications, and services that can sense, log, interpret, communicate, process, and act on a variety of information or control devices in the physical world."[20] Others have suggested that IoT should be described through the lens of its integrated component layers – applications, network, devices, and data – as a way to segment and analyze the associated opportunities and policy challenges.

---

[12] U.S. Council for International Business Comment at 2.
[13] Trans-Atlantic Business Council Comment at 2.
[14] *See, e.g.*, Dr. Cees J.M. Lanting Comment at 4; Dr. Robert Marcus Comment at 26.
[15] IBM Comment at 9.
[16] Center for Data Innovation Comment at 8.
[17] Vodafone US Comment at 88.
[18] American Bar Association Section of Science & Technology Law Comment at 15.
[19] Alain Louchez Comment at 2.
[20] NSTAC Report to the President on the Internet of Things (2014), http://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf.

The growing number of sectors deploying IoT devices includes agriculture, defense, energy, entertainment, environmental monitoring, health care, manufacturing/industrial operations, retail, supply chain logistics, transportation, and others. Often included within the purview of IoT are a variety of "smart" applications, such as "Smart Homes," "Smart Cities," and "Smart Infrastructure."[21]

This green paper will continue to use the term Internet of Things as an umbrella term to reference the technological development in which a greatly increasing number of devices are connected to one another and/or to the Internet. This acknowledges the widespread use and general popular acceptance of the term. The term itself is, as pointed out by some commenters, a misnomer, as many of the devices included in the Internet of Things do not use Internet Protocol or in any event may not connect directly to the Internet.[22] At times, the IoT term is more descriptive of the system or network than an actual thing. IoT has become the commonly used term for the technologies and related issues discussed here, and for the sake of simplicity it will be used throughout this paper.[23]

While this paper takes a broad, flexible approach to the definition of IoT, the Department understands that, in some contexts, a consensus technical definition may facilitate policy development and provide value to stakeholders. However, given the large diversity of devices, applications, and technologies captured under the umbrella of IoT, the Department will consider narrowly tailoring its policy inquiries and actions around categories of uses and/or devices rather than on all of IoT.

In the Request for Comment, the Department asked whether IoT should be treated as a single, unified subject or as a collection of specific categories, such as consumer IoT and industrial IoT. Many commenters supported categorizing IoT, particularly regarding concerns over policy issues such as privacy and safety.[24] Commenters pointed out that "industrial IoT," for example, will usually not raise the same privacy concerns as connected consumer devices.[25] Similarly, the cybersecurity requirements necessary for medical devices may not be the same as the cybersecurity requirements for a stereo system.[26] Smart cities merit particular policy attention

[21] Daniel Castro and Jordan Misra, "The Internet of Things," Center for Data Innovation (November 2013), http://www2.datainnovation.org/2013-internet-of-things.pdf.
[22] Kayleen Manwaring and Roger Clarke, Surfing the Third Wave of Computing: A Framework for Research into E-Objects, Computer Law & Security Review 31 (2015) 595.
[23] In this, IoT is similar to "big data," in that the conversations and reports that were sparked by the popularity of the term were and continue to be important, while the term itself is less useful in laying distinct lines around particular technologies, functionalities, or the creation of specific procurement strategies. (*See generally*, Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values, [May 2014].)
[24] *See, e.g.*, Association for Computing Machinery U.S. Public Policy Council Comment at 3; CompTIA Comment at 5-6; State of Illinois Comment at 20; Bugcrowd Comment at 3; Motorola Solutions Comment at 5.
[25] *See* Secure ID Coalition Comment at 2; BSA | The Software Alliance Comment at 5; Center for Data Innovation Comment at 11-12.
[26] Cisco Systems Comment at 25.

due to the investment and cooperation required to help communities realize the benefits of connectivity.[27] Automated or connected vehicles, unmanned aerial systems, and other types of connected devices also require specific, targeted attention due to the unique challenges and requirements that they pose to traditional regulatory frameworks.[28]

The Department recognizes the importance of the missions of other federal agencies in responding to the challenges raised by IoT use in their areas of focus, and applauds the efforts made thus far to meet them. In the event that our terminology differs from that of other agencies, it may be that the differing terminology is appropriate given the context.

### C. Benefits of IoT

From baby monitors to automatic climate control, IoT technologies promise a wide array of safety and efficiency benefits for consumers and businesses alike. While consumer-facing devices – such as exercise trackers, health monitors, and home safety systems – have drawn much of the media attention, Ligado Networks suggested that the most significant value for the U.S. economy is likely to result from enterprise IoT applications, particularly those that focus on industries such as manufacturing, agriculture, and infrastructure.[29] Broken down by industry, the manufacturing sector appears to have the most to gain from the adoption of IoT, with connected factories increasing productivity, optimizing inventory planning, reducing waste, and saving on energy costs and equipment maintenance. Industry is already exploring how connected devices can improve the safety and reliability of complex processes, and can achieve greater energy and operational efficiencies.[30]

Connected devices are becoming a key tool for providing improved information about supply chains, distribution centers, land, and seaports; for tracking environmental and causal factors; and for helping to secure indoor and outdoor facilities. IoT technology can also help companies reimagine their supply chains, identifying inefficiencies or shipping delays, or confirming product integrity from manufacturing plant to a retail store.[31] These devices are also prevalent in process-driven tasks in which instantaneous feedback and control are essential, such as in the energy sector. Businesses can use this improved data to eliminate inefficiencies in industries such as manufacturing, health care, transportation, energy, and retail.[32]

---

[27] Executive Office of the President, Fact Sheet: Administration Announces New "Smart Cities" Initiative to Help Communities Tackle Local Challenges and Improve City Services (September 14, 2015), https://www.whitehouse.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help.

[28] Association of Global Automakers Comment at 3; AT&T Services Comment at 8.

[29] Ligado Networks Comment at 15.

[30] Providence Group Comment at 2.

[31] Verizon Comment at 9; Georgia Institute of Technology, Center for Advanced Communications Policy and Rehabilitation Engineering Research Center for Wireless Technologies Comment at 3.

[32] Zebra Technologies Comment at 10-11; Southern Company Services Comment at 1-2.

IoT technologies will generate data that helps companies make more-informed decisions, which in turn can improve efficiency, productivity, management, and quality control, regardless of the industry. For example, during transcontinental flights, the sensors on a commercial aircraft's various systems can generate data to improve safety and flight handling.[33] Telematic sensors in tens of thousands of delivery vehicles track engine performance, improve routing, and reduce fuel consumption and overall emissions.[34] Operators in a manufacturing facility with robotic assembly lines can automatically track every action down to the number of times a screw is turned. Any problems can be addressed as they are detected, which minimizes the impact on production.

Consumers are likely to see benefits from IoT in their homes. The Consumer Technology Association suggested that from the consumer perspective, Internet-enabled appliances, home automation components, and energy management devices are moving us toward a vision of the "smart home," offering more security, energy efficiency, and convenience.[35] As the Alliance of Automobile Manufacturers noted in its comments, advancements in vehicle sensors, communications technology, and vehicle automation have the potential to significantly reduce the occurrence or severity of crashes by helping correct for errors in human driving.[36]

Wearable fitness and health monitoring devices and network-enabled medical devices are expected to transform health care, according to the Direct Marketing Association.[37] Through remote health and education services, IoT technology holds immense promise for disadvantaged and rural communities. Connecting medical devices could greatly improve the quality and effectiveness of service, while also expanding the reach of medical professionals and reducing costs. For example, the GSM Association suggested that IoT-enabled remote health monitoring allows medical professionals to facilitate early interventions, improve adherence to medical regimes, and reduce readmission rates.[38] The Internet Society stated that IoT will be beneficial for people with disabilities and the elderly, improving levels of independence and quality of life at a reasonable cost by reducing the number of in-person visits needed to provide the required care.[39]

IoT benefits are not confined to the business and consumer world. Streamlined data and analysis will also enable governments to deliver better, cheaper, and more efficient public services. The improvements suggested in emergency response and first responder capabilities alone are highly encouraging, such as increased collection and sharing of data among first responders. Further, many IoT infrastructure improvements have the ability to provide governments with cross-

[33] BSA | The Software Alliance Comment at 4.
[34] Id. at 4.
[35] Consumer Technology Association Comment at 3; National Association of Realtors Comment at 1.
[36] Alliance of Automobile Manufacturers Comment at 5; Future of Privacy Forum Comment at 5, 18.
[37] Direct Marketing Association Comment at 2.
[38] GSM Association Comment at 18.
[39] Internet Society Comment at 8.

cutting solutions. For example, according to the Future of Privacy Forum, sensors on roads and in traffic signals can allow for dynamic toll pricing and traffic control to decrease congestion.[40] Additionally, the Forum noted, these automated sensors can turn street lights on and off based on street use, potentially reducing both energy consumption and electricity costs.[41] Connected devices can pinpoint costly leaks in water pipes, identify overflowing storm drains that threaten to mix public water with sewage, or detect the area of a power outage quickly without relying on reports from human observers. These devices can also help residents better understand their power or water usage, which may spur them to conserve use and help decrease their utility costs.[42]

Cross-cutting IoT infrastructure advancements have the ability to improve countless government services. From Wi-Fi-enabled trash cans that inform waste management services when they are full in order to increase route efficiency and decrease fuel consumption, to IoT-enabled hospitals and emergency vehicles that can reduce wait times for medical services. BSA | The Software Alliance forecast in its comment that these types of IoT "smart city" initiatives will have an economic impact of up to $1.6 trillion per year by 2025.[43]

A key function of government at all levels, according to the Internet Society, is also to provide for the safety and security of its citizens, and the potential benefits of a robust IoT environment to improve public safety are well documented across law enforcement, fire services, emergency medical services, and homeland and border security.[44] Wearable sensors, body cameras, drones, and Global Positioning System (GPS) trackers are a few examples of technologies being deployed in the field today. Such devices will increase situational awareness to save lives, improve operational efficiency to lower costs, and enable predictive analytics to identify future public safety situations. Additionally, the proliferation of sensors and predictive analytics used by public safety practitioners will benefit citizens by providing real-time access to better information before disaster strikes, which will help people stay safe in emergencies.

## D. Role of Government in Fostering IoT

The goal of this paper is to identify elements of an approach for the Department of Commerce to foster advancement of the Internet of Things, and defers to future policy makers to determine the value of crafting a national strategy. The paper – based on the record of comments received – reviews a range of issues and seeks to set out an approach that should be considered in any future discussions related to a national IoT strategy. According to commenters, any future national

[40] Future of Privacy Forum Comment at 16.
[41] Consumer Technology Association Comment at 3.
[42] *See* Infineon Technologies Americas Comment as 1-2; CTIA Comment at 3-4.
[43] BSA | The Software Alliance Comment at 4 (citations omitted).
[44] Internet Society Comment at 56; Jillisa Bronfman, Weathering the Nest: Privacy Implications of Home Monitoring for the Aging American Population, 208; National Emergency Number Association, National Association of State 9-1-1 Administrators Comment at 2.

strategy, if created, should strive toward global consistency and predictability and be based upon robust interagency coordination, public-private collaboration, and international engagement.[45]

The U.S. Government, through numerous administrations, has a long record of promoting technology and innovation, and the Department expects to build on that foundation in our approach to the IoT environment. Dating back at least to the 1997 Framework for Global Electronic Commerce, the U.S. Government has been operating under the principle that the private sector should lead in digital technology advancement.[46] Even where collective action is necessary, the U.S. Government has encouraged multistakeholder approaches and private sector coordination and leadership where possible. When governmental involvement is needed, it should support and enforce a predictable, minimalist, consistent, and simple legal environment for commerce.[47] The Bush Administration, in its National Strategy to Secure Cyberspace (2003), affirmed the policy that the private sector and government must work together through a voluntary, collaborative process to protect the nation's connected infrastructure.[48]

The U.S. Government has long recognized that innovation can drive economic growth and address national priorities through novel applications of new technologies.[49] The U.S. Government remains committed to the Principles for Internet Policy Making, adopted by the Organization for Economic Cooperation and Development (OECD) in 2011 that stress a flexible, multistakeholder approach to Internet policy making.[50] As the 2011 International Strategy for Cyberspace noted, "connectivity is no end unto itself; it must be supported by a cyberspace that is open to innovation, interoperable the world over, secure enough to earn people's trust, and reliable enough to support their work."[51] Those concepts remain critical to our mission.

Commenters have urged the U.S. Government to avoid over-regulation that could stifle IoT innovation.[52] The risk of premature and excessive regulation is notable given the size of the potential economic benefits to U.S. producers and consumers. Importantly, the U.S.

---

[45] Trans-Atlantic Business Council Comment at 4; Center for Data Innovation Comment at 26; Semiconductor Industry Association Comment at 1l; Rapid7 Comment at 12.
[46] The Framework for Global Electronic Commerce (July 1997), https://clinton4.nara.gov/WH/New/Commerce/.
[47] Ibid.
[48] Executive Office of the President, National Strategy to Secure Cyberspace (February 2003), https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf
[49] Executive Office of the President, A Strategy for American Innovation (October 2015), https://www.whitehouse.gov/sites/default/files/strategy_for_american_innovation_october_2015.pdf.
[50] OECD, OECD Principles for Internet Policy Making (2014), https://www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf
[51] Executive Office of the President, International Strategy for Cyberspace (May 2011), 25, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
[52] Niskanen Center Comment at 9; Alliance of Automobile Manufacturers Comment at 9-10; U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 17.

Government's relevance is not only as a potential policymaker and regulator, but also as an enabler and adopter of IoT technology.[53]

Several commenters called for a national strategy on IoT. As stated by the Center for Digital Innovation:

> A national strategy for the Internet of Things, if designed and implemented correctly, would maximize the opportunity for the Internet of Things to deliver substantial social and economic benefits. The United States will not successfully capture these benefits by leaving development of the Internet of Things solely up to the market, just as no government actions could capture all of the potential benefits without a robust private sector that can innovate unencumbered by overly restrictive regulations.[54]

The Semiconductor Industry Association commented that the "U.S. government should work with industry to establish a long-term national strategy that will enable America to lead the world in IoT ... that promotes key capabilities, including connectivity and interoperability, scalability and security, and complex intelligent analytics."[55] Rapid7 called for "a national strategy with a set of overarching, high-level, voluntary principles generally accepted by government agencies and industry, which IoT security guidelines should follow … [and can] enhance coordination and give agencies, regulated entities, and consumers a roadmap to incentivize development, awareness, and adoption of IoT security standards."[56]

Although no commenters opposed a national strategy, one cautioned that an overly prescriptive technology policy such as that seen in some parts of Asia and Europe could actually disadvantage American competitors as they seek to sell their IoT products worldwide.[57] The GSM Association urged the U.S. Government to focus on spurring IoT adoption and filling gaps that might hinder deployment if left entirely to market forces.[58]

#### i. International Engagement

Those who commented on international engagement expressed the critical importance of a global free and open Internet to future innovation and growth in the IoT space.[59] On IoT issues internationally, the U.S. Government will need to maintain its robust advocacy for industry-led approaches and consensus-based standards and continue to use multistakeholder approaches to

[53] Trans-Atlantic Business Council Comment at 4.
[54] Center for Data Innovation Comment at 26.
[55] Semiconductor Industry Association Comment at 1.
[56] Rapid7 Comment at 12.
[57] Id. at 12.
[58] GSM Association Comment at 7.
[59] Internet Architecture Board Comment at 4; Computer & Communications Industry Association Comment at 6; Center for Data Innovation Comment at 23-24.

address policy challenges. Comments encouraging international engagements fell across a continuum of activities, including engagements focused on breaking down trade barriers, ensuring a consistent approach and common policy approach, and establishing formal IoT dialogues with interested parties.[60] The U.S. Government already has several formal government-to-government dialogues with some of our top trading partners that include digital economy issues. Within these existing dialogues, stakeholders commonly discuss issues such as cross-border data flows, technical standards, privacy, cybersecurity, spectrum allocation, IPv6, and cloud computing. The Department of Commerce expects IoT and related issues to be on the agenda of these international dialogues, and will support continued IoT engagement internationally, through various fora.

There is a wide variety of regional and international entities engaged in standards development related to IoT whose work, and work methods, are critical to the successful implementation of IoT policies. The Department will continue to support U.S. industry initiatives and participation in a range of standards bodies, and will actively advocate for work methods that recognize the value of private sector standardization efforts, and will continue to support greater collaboration between standards organizations. The Department will also advocate against attempts by governments to impose top-down, technology-specific "solutions" to IoT standardization needs.

The effects of varying policies and practices of countries around the world relating to IoT will almost certainly impact U.S. industry competitiveness. The Department of Commerce is aware that several governments recently released national policies and strategies related to the development of IoT. Regardless of whether the U.S. adopts an IoT national strategy, the government plays an important role in articulating and encouraging an approach to IoT policy and standards development worldwide that promotes a globally connected, open, and interoperable IoT environment.

### ii. Stakeholder-Driven Policy Processes

In addition to its role advocating internationally for policies that are conducive to IoT advancement and balanced global policy, some commenters also noted that the U.S. Government can continue to play a role in convening public-private processes to address policy challenges in the IoT arena. Commenters acknowledged the success of the Department's efforts to engage with stakeholders, including civil society and the private sector, in building flexible and adaptable frameworks, codes of conduct, and best practices in the fast-moving technology policy space.[61] Examples include the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Multistakeholder Forum on the Digital Millennium Copyright Act (DMCA)

[60] Microsoft Comment at 16; Symantec Comment at 5; U.S. Council for International Business Comment at 7.
[61] CA Technologies Comment at 5; Family Online Safety Institute Comment at 4-5; CTIA Comment at 16; Internet Commerce Coalition Comment at 1, 4; Software & Information Industry Association Comment at 7; Cisco Systems Comment at 1, 13; AT&T Services Comment at 4, 28-9.

Notice and Takedown System, convened by the U.S. Patent and Trademark Office (USPTO) and the National Telecommunications and Information Administration (NTIA).[62] Commenters noted that the U.S. Government should continue to employ these processes to solve policy challenges as an alternative to pursuing top-down regulatory solutions while IoT technologies are still advancing and gaining market scale.[63]

## 3. An Approach for Departmental Action to Advance the Internet of Things

Given the great economic and social potential of IoT, as well as the qualitatively different challenges raised by its development, it is important for the Department to engage proactively yet selectively on issues described in this paper.

The Department has a longstanding approach to encouraging innovation in new technologies, while taking steps to address policy matters in a proactive, multistakeholder manner. We have approached emerging market trends and technologies with restraint and an eye toward allowing new entrants room to experiment and mature before they encounter significant government intervention. These guiding principles worked well as the Internet developed, and – as gleaned from our commenters – are appropriate to apply in the IoT sphere as well. Coupled with close partnership and collaboration with stakeholders, including our government and international partners, a cautious but thoughtful approach will map well to an emerging landscape where existing and new policy and technology norms and standards are starting to coalesce or collide. The overarching goal will remain the same: to foster the benefits of IoT while meeting its challenges.

**Figure 1. The Department of Commerce will work across multiple stakeholder communities to foster IoT advancement.**


[62] *See* NIST, Framework for Improving Critical Infrastructure Cybersecurity, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf. For information on the Forum, *see* https://www.uspto.gov/learning-and-resources/ip-policy/copyright/multistakeholder-forum-dmca-notice-and-takedown-system.

[63] *See* ADP Comment at 3; General Motors Comment at 3; U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 3-4.

Several principles – derived from stakeholder input – will guide the Department's intended ongoing engagement with all stakeholders at the local, tribal, state, federal, and international levels across the evolving IoT landscape.

- ❖ The Department will lead efforts to ensure the IoT environment **is inclusive and widely accessible** to consumers, workers, and businesses;
- ❖ The Department will recommend policy and take action to support a **stable, secure, and trustworthy** IoT environment;
- ❖ The Department will advocate for and defend a **globally connected, open, and interoperable** IoT environment built upon industry-driven, consensus-based standards; and
- ❖ The Department will encourage IoT **growth and innovation** by encouraging expanding markets and reducing barriers to entry, and by convening stakeholders to address public policy challenges.

We have identified four broad areas of engagement:

- **Enabling Infrastructure Availability and Access:** Fostering the physical and spectrum-related assets needed to support IoT growth and advancement.
- **Crafting Balanced Policy and Building Coalitions:** Removing barriers and encouraging coordination and collaboration; influencing, analyzing, devising, and promoting norms and practices that will protect IoT users while encouraging growth, advancement, and applicability of IoT technologies.
- **Promoting Standards and Technology Advancement:** Ensuring that the necessary technical standards are developed and in place to support global IoT interoperability and that the technical applications and devices to support IoT continue to advance.
- **Encouraging Markets:** Promoting the advancement of IoT through Department usage, application, iterative enhancement, and novel usage of the technologies; and translating the economic benefits and opportunities of IoT to foreign partners.

We expect to work on a set of cross-cutting issues across these contexts from cybersecurity and privacy to innovation and intellectual property, with all stakeholders, at the local, tribal, state, federal, and international levels. The next section delves in depth into each of these areas of engagement, summarizing commenter feedback, describing current Department initiatives, and proposing next steps.

## 4. Areas of Engagement

As detailed below, the Department plans to work on IoT matters – with both ongoing and new activities – across a range of contexts.

### A. Enabling Infrastructure Availability and Access

The expected increase in connected devices associated with IoT will dramatically increase demands upon the nation's information and communications infrastructure.[64] It could put stress on legacy networks as well as more recently deployed all-Internet Protocol systems.[65]

#### i. Increased Infrastructure Demand

IoT will depend upon both public and private communications networks, and will use various wireline and wireless modes, including satellite, often in combination or on an interdependent basis.[66] For example, different network resources may be used for access or backhaul, or to off-load traffic. The need for seamless connectivity will require deployment of robust broadband infrastructure for interconnecting devices.[67] Cisco estimates that, in addition to the anticipated expansion in the number of devices, Internet traffic will be 22 times greater in 2018 than 2013.[68] Such traffic growth is likely to dictate the need for greater overall network capacity – and smarter use of the bandwidth that is available.

Meeting these connectivity demands will require continued modernization of legacy telecommunications infrastructure and buildout of additional broadband capable networks. A percentage of the current telecommunications networks were primarily built for voice service and historically were largely copper-based. Over time, however, the demand for other services, including broadband Internet access, and more recently, video applications, has helped to fuel a transition to all-Internet Protocol-based multimedia networks using a variety of technologies such as fiber, hybrid fiber-coaxial cable, enhanced copper, and wireless networks that offer increased capacities. This transformation is allowing for much more dynamic, more efficient, and faster means of connecting devices. As a result, ongoing and future efforts across the country to spur increased broadband deployment and adoption should have a positive multiplier effect on IoT usage and functionality. Commenters did express concerns regarding hurdles to deploying infrastructure, including difficulties in siting of wireless towers and antennas, and access to

[64] *See* Competitive Carriers Association Comment at 2-3; Mobile Future Comment at 1.
[65] University Corporation for Advanced Internet Development Comment at 11.
[66] Inmarsat Comment at 2; Ligado Networks Comment at 6; Satellite Industry Association Comment at 1-2; Hughes Network Systems Comment at 1.
[67] United States Telecom Association Comment at 3-4 (citations omitted).
[68] Cisco Systems Comment at 17.

necessary poles, conduits, and rights-of-way.[69] With wireless networks, these problems are exacerbated by emerging architectures that require significantly more infrastructure than legacy systems.

### ii. Increased Spectrum Demand

Wireless technologies are likely to play a significant role in supporting many of the increasing numbers of connected devices being developed by IoT manufacturers. In addition to existing wireless resources, IoT applications will leverage exciting technological advances, such as those associated with 5th generation (5G) wireless technologies, innovative unlicensed use of spectrum, low-power connectivity protocols, and others. Many commenters, however, pointed out that a shortage of available spectrum could become a constraint on the growth of IoT.[70]

IoT-associated demand for spectrum access is rapidly expanding, from consumer-focused applications, to industrial systems to increasing government use cases. For example, Qualcomm pointed out that automated vehicles, critical infrastructure management, remote medical procedures, and command and control communications for unmanned aerial vehicles and robotics may all use different spectrum bands.[71] Hewlett Packard Enterprise similarly commented that the expected diversity in connected devices and applications means that the required data rates as well as the duration and persistence of transmissions will vary widely, meaning that spectrum needs will be very different depending on the device and application.[72]

Some commenters asserted the need for dedicated spectrum to support connected automobiles.[73] Today, automobiles already rely on connectivity for safety, convenience, and entertainment features. This trend is expanding, highlighted by the development of autonomous vehicles, and multiple communications technologies are likely to play a role.

Spectrum will also play a key role in the ability of utilities to leverage IoT technologies, according to the Edison Electric Institute. It also noted that utilities seek dedicated spectrum for broadband communications to manage peak loads, maintain grid stability, and monitor and control millions of utility system devices.[74] Deere & Company observed that many IoT systems, including those in agriculture, rely on unimpaired location services. As a result, Deere urged that government spectrum policies continue to protect the GPS from harmful interference.[75]

---

[69] Wireless Infrastructure Association Comment at 2; Mobile Future Comment at 16; IoT Policy Network Comment at 8.
[70] Competitive Carriers Association Comment at 16; Consumer Technology Association Comment at 9-10; Semiconductor Industry Association Comment at 2; Karim Farhat Comment at 2.
[71] Qualcomm Comment at i.
[72] Hewlett Packard Enterprise Comment at 3.
[73] *See* General Motors Comment at 8-9; Alliance of Automobile Manufacturers at 7-8.
[74] Edison Electric Institute Comment at 6.
[75] Deere & Company Comment at 8.

IoT devices and applications will rely on various wireless technologies in rapidly escalating numbers, and they will use a number of licensed and unlicensed spectrum bands. This will increase demands on already scarce wireless spectrum resources.[76]

As a result, commenters generally agreed that the U.S. Government can advance IoT by ensuring that our limited spectrum resources are used effectively and efficiently.[77] Many suggested that access to additional spectrum will be needed to support IoT,[78] with support for a balance between licensed and unlicensed access.[79] Some indicated that specific spectrum bands should be identified that could support IoT with some flexibility in exactly how such spectrum is used.[80] Many other commenters, however, recommended the federal government instead maintain its overall approach of meeting increasing demand by continuing to make available a broad range of spectrum on a technology neutral, flexible-use basis.[81] AT&T commented that, for licensed spectrum, the licensee can manage and employ the spectrum it controls in an optimized fashion for the mix of traffic types that it needs to support.[82] It also stated that such flexible commercial spectrum allocations allow the evolving market and consumers to determine the highest and best use of the spectrum and affords an opportunity for innovative technologies to emerge.[83]

Commenters noted that the wireless industry requires access to a broad range of frequencies across the lower, middle, and higher spectrum bands to support enhanced connectivity for consumer, enterprise, and other uses, including IoT.[84] Some commenters urged the U.S. Government to encourage policies that ensure competitive carriers and small providers have access to additional licensed spectrum.[85] Hewlett Packard Enterprises suggested that dynamic sharing mechanisms and spectrum access systems may hold great promise for unlocking access to spectrum, particularly in sub-1 GHz bands, adding that the lack of spectrum availability in these bands is a potential constraint on the growth of IoT.[86] The Wi-Fi Alliance echoed this call for unlicensed access to spectrum in lower frequency bands.[87]

[76] IoT Policy Network Comment at 8; State of Illinois Comment at 15; the U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 9.
[77] CTIA Comment at 14; Mobile Future Comment at 2; Ligado Networks Comment at 9; U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 10.
[78] 5G Americas Comment at 6; Consumer Technology Association Comment at 9-10.
[79] Verizon Comment at 12-13.
[80] IEEE-USA Comment at 2; ARM Comment at 6-7; Hewlett Packard Enterprise Comment at 2.
[81] CTIA Comment at 14; 5G Americas Comment at 5-6; CompTIA Comment at 2-3; Telecommunications Industry Association Comment at 8; Silver Spring Networks Comment at 2-3.
[82] AT&T Services Comment at 34-35.
[83] CTIA Comment at 14; CompTIA Comment at 4.
[84] Ligado Networks Comment at 13; Qualcomm Comment at 14; T-Mobile USA Comment at 15.
[85] Competitive Carriers Association Comment at 4-5; Ligado Networks Comment at 20.
[86] Hewlett Packard Enterprise Comment at 2.
[87] Wi-Fi Alliance Comment at 7.

### iii. Internet Protocol Version 6 Adoption

There is a growing demand for Internet connectivity in light of IoT. Many devices connect to the Internet via Internet Protocol addresses (IP addresses). The system most in use today – Internet Protocol version 4 (IPv4) – was created in the 1970s as the Internet's first, large-scale addressing system, and it provided us with nearly 4.3 billion IP addresses. This number, however, is far less than what the ever-expanding network – and IoT – will demand. As one commenter noted, IPv4 is an "outdated version of the Internet Protocol" which "severely restricts the number of devices that can be connected to the Internet."[88]

In the 1990s, the Internet technical community provided a sustainable solution to this problem by creating IPv6, the next generation protocol. IPv6 offers a significantly expanded addressing space that can comfortably meet the growing demand for Internet connections and obviate the need for technologies used to prolong the life of IPv4. Compared with IPv4's 4.3 billion possible addresses, IPv6 offers 340 trillion trillion trillion addresses.

Although IPv6 addresses are available and plentiful, the majority of the Internet has not made the transition from IPv4 to IPv6.[89] Thus, a key question is what incentives or policy approaches can help quicken the pace of IPv6 adoption, in order to create the optimal enabling environment for the sustainable growth of IoT.[90] Due in large part to IoT, billions of additional devices – from industrial sensors to home appliances and vehicles – will be connected to the Internet between now and 2025.[91] Commenters point out that the expected increase in connected devices associated with IoT will dramatically increase demands upon the nation's information and communications infrastructure,[92] and that "only IPv6 will scale to the size expected for Internet communication."[93]

---

[88] Internet2 Comment at 2.

[89] Continued use of IPv4 is made possible through technologies like "Network Address Translation" (NAT), which can be used to stretch dwindling IPv4 resources by allowing several devices or Things to share one IP address. Some view these technologies as only a temporary fix for the unavoidable problem of "IPv4 exhaustion." This is due in large part to the different costs associated with doing so, for example the purchasing of new hardware, or the time needed to train employees and plan deployment. For many, without an understanding of the opportunities that it provides and the ultimate necessity for its adoption, the day-to-day costs of running a business will take precedence over long-term investment in IPv6, which can require a multi-year planning and testing process. Moreover, with technologies like NAT, businesses can continue to defer IPv6 implementation. Finally, for those businesses that do not provide ICT services but depend on them – especially SMEs – IPv4 exhaustion might be a scantily understood or even unknown issue.

[90] NTIA put out a Request for Comment on developing initiatives to increase IPv6 adoption in August, 2016. See NTIA Request for Comments on the Incentives, Benefits, Costs, and Challenges to IPv6 Implementation (18 August 2016), available at: https://www.ntia.doc.gov/federal-register-notice/2016/incentives-benefits-costs-and-challenges-ipv6-implementation-0.

[91] ISOC, "The Internet of Things: An Overview" Comment at 23.

[92] Competitive Carriers Association Comment at 2-3; Mobile Future Comment at 1.

[93] Internet Architecture Board Comment at 3.

At the same time, however, one comment noted that IPv6 implementation requires many considerations, including security concerns generated by the capabilities of devices connected to the network. "Unlike IPv4, which was relatively simple to implement, IPv6 is more complicated," Krawetz, et al, noted. "Many IoT devices do not fully implement IPv6. These incomplete implementations are vulnerable to network attacks and malware."[94] The capacity of hardware and software to support IPv6 is one of several considerations to take into account when deploying IPv6 services. Despite this challenge and others, the Internet Society stated, many experts believe that IPv6 is "the best connectivity option and will allow IoT to reach its potential."[95] In support of this effort, the Department will continue to encourage the adoption of IPv6 through its ongoing efforts to enhance standards profiles, support measurement and testing infrastructures, and foster multistakeholder collaboration.

### iv. Issues of Equity in IoT

Connected devices have the extraordinary potential to improve the health, economic, and personal welfare of underserved communities. Wearable devices can closely monitor a patient's health, which is critical for certain illnesses. Heath care providers can do this remotely, which helps rural patients or patients with mobility problems. Because of this, it is essential that government and the private sector work together to ensure that all Americans have an opportunity to reap the benefits brought by IoT.

While IoT has the ability to improve the lives of consumers and citizens, a lack of access to the Internet, and thus many IoT applications, could also make things worse for underserved communities. The Center for Data Innovation commented that if "the public sector does not implement policies to encourage equitable deployment, the Internet of Things could exacerbate existing inequalities by providing the benefits of data-driven decision making only to some, and placing already underserved communities at an even greater disadvantage."[96] In general, the concern is the cumulative impact of inequality (e.g., economic status plus other factors), and how some consumers may be left out of the benefits of IoT. The growth in IoT device use and the resulting data analytics from their use has been significant, and government should be conscious of issues of social inclusion and equity.[97]

### v. Planned Activities

It is clear from commenters that infrastructure needs to be deployed, developed, and maintained to ensure that IoT reaches its full potential. This will require a continued focus on the deployment of, and investment, in wireline and wireless connectivity, spectrum availability, and

[94] Neal Krawetz, Eric Schultz, Valerie Kaminsky, Bill Tucker, et al. at 15
[95] Internet Society Comment at 27.
[96] Center for Data Innovation Comment at 7.
[97] White House, *Big Data: Seizing Opportunities, Preserving Values* (May 2014), https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.

standards development. The push for infrastructure deployment and development should be private-sector led, with the support of the Department to assess spectrum requirements, promote and foster broadband deployment, and ensure that access is made available to all communities. IoT infrastructure development will also require international engagement to address issues of interoperability, access, and inclusiveness.

### *1. Current Initiatives*

- **Empowering Communities to Become Smart Cities.** NTIA assists in the development of the broadband infrastructure necessary for the use of IoT both directly through toolkits and indirectly through work with the Broadband Opportunities Council (BOC). Private-sector partners can be an important source of capital, technical knowledge, continuing innovation, and workforce development. To assist communities looking to embed new digital technologies into municipal infrastructure, NTIA released Using Partnerships to Power a Smart City: A Toolkit for Local Communities for local officials and citizen groups to use as a guide for building successful public-private partnerships.[98] The Department co-chairs the BOC, which includes 25 federal agencies and departments and that engages with industry and other stakeholders to understand ways the Executive Branch can better support the needs of communities seeking broadband investment. The BOC released a report in September 2015 that includes action items and milestones for each agency, and will continue its work to monitor implementation of the action items and to explore additional steps that can be taken to remove barriers to broadband deployment and adoption.[99]

- **Research and Development into Spectrum-Related Interactions.** NTIA's Institute for Telecommunication Sciences (ITS) is investigating interaction effects among new IoT-related spectrum use and incumbent spectrum users in cases where they are collocated and/or in adjacent bands. This is creating a technically neutral body of knowledge and expertise to inform future policy. Continued development of this IoT testbed will provide a better understanding of the performance and behavior of IoT systems. It will also establish a base of scientific principles to inform neutral and accurate predictions of future spectrum needs and trouble areas. Using the scientific principles derived by the continued development of the IoT testbed, ITS also plans to develop the capability to model large-scale interactions of currently deployed and new, not-yet deployed IoT systems.

[98] Using Partnerships to Power a Smart City: A Toolkit for Local Communities, https://www2.ntia.doc.gov/files/smartcities-toolkit_111516_v2.pdf.
[99] Broadband Opportunity Council Report and Recommendations, https://www.whitehouse.gov/sites/default/files/broadband_opportunity_council_report_final.pdf.

- **Enabling IoT Functionality for First Responders.** An anticipated key driver of the benefits of IoT for public safety is the First Responder Network Authority's (FirstNet) Nationwide Public Safety Broadband Network (NPSBN). FirstNet is deploying the necessary infrastructure to allow for transfers of data wirelessly, real-time in the field, without potential congestion from commercial network traffic. This will be crucial during routine day-to-day incidents, large planned events or unexpected disasters. In 2012, Congress allocated $7 billion and 20 megahertz of spectrum to FirstNet to partner with the private sector to build the NPSBN, an LTE-based wireless broadband network dedicated to public safety. Once operational, the FirstNet network promises to transform the way first responders communicate, providing public safety personnel with dedicated access over a prioritized, reliable, and secure mobile connection. This will enable first responders to send and receive text, voice, video, images, location information, and other data in real time to help increase situational awareness and operational capability in the field.

  In addition to revolutionizing emergency communications, the FirstNet network will be an incubator and proving ground for public safety focused IoT solutions by linking more first responder data sources, such as their gear, emergency vehicles, fingerprint scanners, databases, and more. The constant transfer of data over a dedicated, mission critical network will enable faster decision making that can help coordinate responses and save lives. By focusing on public safety needs first, FirstNet seeks to drive industry to continue to innovate to improve public safety activity to save lives, improve responses to incidents and disasters, and better anticipate future responses.

- **IPv6 Adoption.** The Department is championing IPv6 adoption and use in networks, devices, and websites, and promoting more IPv6-enabled content, but there is more to be done. NIST leads IPv6 planning within the U.S. Government, and developed the technical infrastructure to assist the Government with IPv6 adoption.[100] NTIA and NIST have in the past supported awareness-raising and information-sharing by holding public meetings on IPv6,[101] and have produced informational resources to help those implementing the new protocol, including a *Technical and Economic Assessment of IPv6* (2006) and an *IPv6 Readiness Tool for Business* (2011).[102] NIST leads IPv6 planning within the U.S. Government, and developed the technical infrastructure (i.e., standards profiles, testing infrastructure, and deployment guidance) to assist the government with

[100] See the NIST Information Technology Laboratory, Advanced Network Technologies Division website, available at https://www-x.antd.nist.gov/usgv6/.
[101] NTIA and NIST have held two public workshops on IPv6 (2004, 2010), https://www.ntia.doc.gov/federal-register-notice/2004/notice-public-meeting-ipv6; https://www.ntia.doc.gov/page/ipv6-workshop-09282010.
[102] These resources and more are available on NTIA's website, https://www.ntia.doc.gov/page/additional-ipv6-resources.

IPv6 adoption.[103] The agency also maintains up-to-date statistics on IPv6 deployment.[104] NTIA conducted a Request for Comment (RFC) on the *Incentives, Benefits, Costs and Challenges to IPv6 Implementation* in order to better understand the industry's experience with and viewpoints on IPv6 implementation, and received a number of high quality insights from individuals, cloud providers, Internet service providers, and various industry associations.[105]

### 2. Proposed Next Steps

The Department will:

- Coordinate with the private sector, as well as federal, state, and local government partners, to ensure the infrastructure to support IoT continues to expand, that access to infrastructure is inclusive and affordable, and that the infrastructure remains innovative, open, secure, interoperable and stable. This includes promoting adoption and usage to encourage deployment and investment, and engaging in technical assistance and research and development.

- Continue to innovate in spectrum management to increase access to spectrum that will help facilitate IoT growth and advancement. NTIA, through its Office of Spectrum Management, will collaborate with stakeholders, including its spectrum-related interagency (Policy and Plans Steering Group and Interdepartmental Radio Advisory Committee) and external advisory bodies (Commerce Spectrum Management Advisory Committee), to assess the spectrum implications of the diverse IoT applications that currently or in the future may be delivered through a number of technologies operating in various spectrum bands.

- Expand its digital inclusion efforts to include an emphasis on IoT adoption and availability.

- Continue to encourage the adoption of IPv6 by fostering multistakeholder collaboration and dialogue and provide a platform for discussion on issues such as mobile IPv6 routing, security in dual-stack environments, and privacy implications of IPv6.

[103] See the NIST Information Technology Laboratory, Advanced Network Technologies Division website, available at https://www-x.antd.nist.gov/usgv6/.
[104] https://usgv6-deploymon.antd.nist.gov/cgi-bin/generate-gov.
[105] NTIA Request for Comments on the Incentives, Benefits, Costs, and Challenges to IPv6 Implementation (18 August 2016), available at: https://www.ntia.doc.gov/federal-register-notice/2016/incentives-benefits-costs-and-challenges-ipv6-implementation-0.

- Collect data and conduct analysis on the usage and growth of IoT devices through its Digital Nation data collection in order to better inform industry and policy makers.

## B. Crafting Balanced Policy and Building Coalitions

Commenters detailed several discrete policy areas that will require coordinated engagement by all stakeholders – government, civil society, academia, the technical community, and the private sector, globally and domestically – to ensure forward-looking, adaptable, and balanced policy that fosters innovation while addressing risks and challenges.

### i. Cybersecurity

IoT will be integrated into our lives to an unprecedented degree. While the computer and Internet revolutions have pushed more of our lives into the data domain, IoT will continue that trend and bring both software and connectivity into almost every aspect of the home, enterprise, and public space. One comment noted that several factors contribute to the more challenging environment of increased connectivity, including: the highly networked nature of IoT creates a large number of attack surfaces that can be exploited; some IoT device makers have not followed established cybersecurity best practices used in other information security contexts; and some connected devices will collect vast amounts of personal information, enabling high impact attacks.[106]

Meanwhile, the expected ubiquity of and dependence on IoT magnifies the security risk on each domain, whether it is the power grid, our automobiles, or children's toys. The distributed denial of service (DDOS) attack in October 2016 on a Domain Name Service (DNS) provider's lookup service that used an army of IoT devices protected only by factory-default passwords is an example of how Internet-connected devices have changed the cybersecurity environment.[107] The incident was the most visible and far-reaching example of the potential risks that must be mitigated when considering IoT. Incident management in cases such as these may require enhanced coordination by the private sector, government, and individuals in the future.

The risks for IoT systems that support the economy's industrial sectors are even more challenging, according to IBM. Industrial devices are connected to the Internet to allow for broader visibility, control, and maintenance, but these devices can also become potential attack targets.[108]

At the same time, commenters noted that cybersecurity best practices are a new concept for many IoT stakeholders. Mature manufacturers of newly wired devices, such as an appliance manufacturer developing a wireless-enabled refrigerator, may have little to no experience

[106] ABA Section of Science &Technology Law Comment at 11.
[107] Brian Krebs, Hacked Cameras, DVRs Powered Today's Massive Internet Outage, Krebs on Security (October 21, 2016), https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/.
[108] IBM Comment at 5.

collecting, securing, and protecting consumer data, the Electronic Frontier Foundation (EFF) said in its comments.[109] EFF added that start-ups building IoT technologies and interfaces for the first time may focus primarily on getting a product to market, without considering how to protect and secure computer networks or data.[110] Commenters stated that different sets of best practices will be relevant for different IoT entities, such as hardware manufacturers/integrators, developers, deployers, and operators.[111]

### 1. Need for Flexible, Risk-based Solutions

Threats and vulnerabilities are constantly evolving. Predefined solutions quickly become obsolete or even provide bad actors with a roadmap for attack, the U.S. Chamber of Commerce noted.[112] Many commenters stated that regulators must allow developers the flexibility to create cutting-edge improvements to defend their products and services and protect their users.[113] Overly prescriptive regulations could impede stakeholders' abilities to respond to ever-changing threats, AT&T commented.[114] Cisco stated that governments should work within existing regulatory structures, and focus on outcome-oriented approaches to manage newly identified risks associated with the use of particular technologies, instead of regulating the underlying technologies.[115]

The U.S. Government can play a valuable role in driving awareness and resolution of the cybersecurity issues facing IoT development, Rapid7 wrote, suggesting the government can facilitate coordination and standardization among IoT stakeholders to improve security.[116] Several commenters called for a greater recognition of the role played by the security research community, which can independently discover, assess, and correct cybersecurity vulnerabilities.[117]

Commenters recommended that the U.S. Government continue to foster a community for cybersecurity information sharing, and collaborate with industry on clearer guidelines for security research and coordinated disclosure.[118] The Information Technology Industry Council pointed to two examples of public-private partnerships that can help ensure greater coordination

[109] Electronic Frontier Foundation Comment at 5.
[110] *Ibid.*
[111] *See* Microsoft Comment at 7; Information Technology Industry Council Comment at 8; Software & Information Industry Association Comment at 2.
[112] U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 13.
[113] *See* Application Developers Alliance Comment at 4; AT&T Services Comment at 45; Cisco Systems Comment at 22-23.
[114] AT&T Services Comment at 45.
[115] Cisco Systems Comment at 23.
[116] Rapid7 Comment at 8-9.
[117] *See* Access Now Comment at 8; Rapid7 Comment at 6; ACM U.S. Public Policy Council Comment at 5.
[118] *See* IBM Comment at 14; Access Now Comment at 7; U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 14.

and collaboration across the government: information sharing and analysis centers and sector coordinating councils.[119]

Commenters suggested some limited areas that may require special consideration. Devices that are used by children may constitute one of these areas.[120] For example, as Common Sense Kids Action pointed out, a recent data breach involving a toy manufacturer exposed names, dates of birth, password recovery questions and answers, genders, pictures of parents and children, audio recordings of children, and chat logs between parents and children.[121] Autonomous vehicles may be another area for special consideration, particularly regarding safety-critical systems. The Association of Global Automakers recommended Federal criminal penalties for those who electronically tamper with a motor vehicle without the owner's consent.[122]

The range of IoT devices and applications, as well as the many potential attack vectors and harms, may preclude a single, prescriptive solution. Instead, many commenters advocated a risk-based approach to understand threats and vulnerabilities.[123] Just as there is no easy description for IoT itself, there is no single prescription for IoT security. Commenters argued that breaking down the security challenge into particular risks allows for a better understanding of the solution space. Symantec, for example, distinguishes between risks to communications to/from an IoT device, and risks that undermine the integrity of the device itself.[124] Many other commenters highlighted the fact that concerns about the risks to data confidentiality and integrity can be best addressed by encryption,[125] while other commenters said that concerns about the risk of malicious control of devices require access control and authorization mechanisms.[126] At the September 2016 IoT workshop, the Providence Group's Dan Caprio stated that IoT risk is such a complex and multifaceted issue that it needs to be addressed through an enterprise risk management approach.[127]

This emphasis on a risk-based approach conforms with a broader focus across the Department on understanding and addressing cybersecurity risks in the business/mission context.[128] This

---

[119] Information Technology Industry Council Comment at 9.
[120] *See* Family Online Safety Institute Comment at 3; Future of Privacy Forum Comment at 10; Common Sense Kids Action Comment at 2; Staff of the Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning Comment at 6.
[121] Common Sense Kids Action Comment at 2-3.
[122] Association of Global Automakers Comment at 5.
[123] Infineon Technologies Americas Comment at 6; the U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 13; Software & Information Industry Association Comment at 9.
[124] Symantec, "An Internet of Things Reference Architecture" Comment at 2, 16.
[125] *See* Internet Association Comment at 6; Telecommunications Industry Association Comment at 13.
[126] *See* Rapid 7 Comment at 12; Samsung Comment (June 2, 2016) at 3.
[127] Fostering the Advancement of the Internet of Things Workshop, September 1, 2016, Transcript, https://www.ntia.doc.gov/files/ntia/publications/09012016-iot-workshop.pdf.
[128] Executive Office of the President, Executive Order – Improving Critical Infrastructure Cybersecurity, February 12, 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

approach is embodied within the NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework). Many commenters referenced the NIST Framework as providing a model to think about cybersecurity for IoT applications and devices.[129] The NIST Framework offers an overarching structure to address cybersecurity across all critical infrastructure sectors using existing international standards and best practices, while providing adaptability and flexibility to meet the unique needs of each sector and address new threats.

The NIST Framework 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 their particular business models, assets, and other variables. This structure enables organizations to adapt to an ever-changing, dynamic environment, which is critical for IoT technologies. Verizon called for a process expanding on NIST's model that builds on collaboration between industry, academic, and government stakeholders to identify standards and practices for IoT security.[130]

### *2. Security by Design*

Many commenters underscored the importance of security considerations as an integral part of the entire life cycle of IoT products, from conception to deployment and beyond. The Software & Information Industry Association, for example, encouraged a practice of a risk assessment during the product design stage and security testing during development and before products and services launch.[131] When integrating multiple components, Rapid7 suggested that each component must be understood well enough to configure it properly to minimize unused features and secure any insecure defaults.[132]

As several commenters noted, a common means of capturing this holistic approach to security is "security by design,"[133] a concept the Department strongly supports.[134] This is not a new idea, and is linked to important concepts like "privacy-by-design."[135] The Federal Trade Commission has also embraced this approach, with its IoT guidance that companies "Start with Security."[136]

---

[129] CTIA Comment at 16; CA Technologies Comment at 5; Coalition for Cybersecurity Policy & Law Comment at 4-5.
[130] Verizon Comment at 20.
[131] Software & Information Industry Association Comment at 9.
[132] Rapid7 Comment at 3-4.
[133] *See, e.g.,* Software & Information Industry Association Comment at 9; Nest Labs Comment at 14; ARM Comment at 5.
[134] *See* remarks of Secretary Penny Pritzker at the U.S. Chamber of Commerce, September 27, 2016. "[A]t the National Telecommunications and Information Administration, we are engaging stakeholders in fast-growing sectors like the 'Internet of Things' to ensure that the cars, home security systems, baby monitors, and devices of the future are born secure."
[135] Software & Information Industry Association Comment at 11; Thierer Comment at 90. For more, see NIST Privacy Engineering program at http://csrc.nist.gov/projects/privacy_engineering/.
[136] Federal Trade Commission, Start With Security: A Guide for Business (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

The overall notion is often most easily understood in its absence: security failures are more likely to occur when security is not a consideration throughout the concept and design process. Attempts to "bolt on" security features late in the product development process are both more expensive and more prone to error.

While many commenters embraced this notion, there is no clear consensus or straightforward path on how to implement such a concept across the broad IoT space. The software industry has spent many years developing tools, techniques, and standards for integrating security into the development lifecycle. These range from approaches developed by specific companies to those developed by open standards organizations.[137] The Information Technology Industry Council suggests starting at the hardware level with built-in safeguards.[138] Other mechanisms for building in security include considering authentication tools, using modern, well-tested software packages, and having a complete testing protocol in place. Designers, developers, and integrators must understand security from an initial stage. Further tools to empower easier security decision-making may be necessary as IoT grows.

The final hurdle to security-by-design is the challenge of how to communicate the effectiveness of security practices to customers, relevant regulators, and the public. This problem is not unique to IoT, but is necessary to foster public trust and market rewards for security investment.

### *3. Patching*

The lifecycle of a device lasts beyond the development process and will vary greatly depending on the device, from short periods to many years. The Electronic Frontier Foundation noted that unpatched smart devices create security vulnerabilities and can put privacy at risk by making devices easier to compromise or by leaking user information.[139] Manufacturers of connected devices, unlike those who make traditional computers, often lack an effective update and upgrade path once the devices leave the manufacturer's warehouse. Several commenters noted that, without a patching capability, it is difficult to mitigate devices' known security flaws on a large scale.[140] These vulnerabilities can have potentially devastating consequences for users.[141]

Many manufacturers entering the IoT space do not traditionally offer frequent or fast-paced support or updates to their products, and are only beginning to look into quick response practices

---

[137] *See, e.g.*, Microsoft (https://www.microsoft.com/en-us/sdl/); Building Security in Maturity Model (https://www.bsimm.com/about/); Software Assurance Maturity Model (https://www.owasp.org/index.php/OWASP_SAMM_Project); NIST Special Publication 800-160 (http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf); ISO/IEC 27034:2011 (http://www.iso27001security.com/html/27034.html).
[138] Information Technology Industry Council Comment at 7.
[139] Electronic Frontier Foundation Comment at 5.
[140] *See* Software & Information Industry Association Comment at 9; Coalition for Cybersecurity Policy & Law Comment at 5; Internet Architecture Board Comment at 3; Rapid7 Comment at 3.
[141] Comment of Association for Computing Machinery, ACM U.S. Public Policy Council at 6.

for vulnerability patching, Rapid7 commented.[142] Effective patching is challenging even for mature market sectors that have update mechanisms, such as smartphones and routers, and therefore Rapid7 suggests IoT newcomers will need to quickly incorporate patching and updating processes into their practices.[143]

Many connected devices are likely to be long-lived (sometimes lasting decades), and many will undoubtedly require patches as security issues are identified in the future. For example, cars are purchased with the expectation that they will be used for at least 11 years.[144] Commenters suggested that methods to allow updates from reputable sources, sometimes despite low bandwidth and intermittent connections especially over the long term, should be considered. This is important even if the original manufacturer or service provider no longer supports the device or is no longer in business.[145] Meanwhile, Microsoft pointed out that many connected devices will be deployed into environments that fall under multiple jurisdictions with different regulatory requirements, or into consumer environments with fewer security management resources.[146]

#### *4. Technical Limitations*

One comment highlighted the technical limitations of many IoT devices as a particular hurdle for implementing known good security practices.[147] These limitations include computationally weak hardware, minimal operating systems, and/or limited memory, commented Krawetz et al. They added that limited resources make connected devices more vulnerable to denial of service and stacksmashing attacks (causing a stack in a computer application or operating system to overflow, which may subvert or crash the stack); the IoT world has not yet developed common mitigation techniques.[148] Even when adequate technology exists, devices may lack the metrics or interfaces for security awareness. CTIA commented that a breach could exist for an extended period of time before being noticed, and once noticed, correction or mitigation may not be possible or practical.[149] Alternative solutions may require greater coordination across different parts of the IoT environment.

The difficulties and costs of implementing encryption on technically limited devices drew substantial comment. Researchers who studied IoT encryption found that many of the devices

[142] Rapid7 Comment at 3.
[143] Id.
[144] *See* http://www.consumerreports.org/cro/2012/05/make-your-car-last-200-000-miles/index.htm
[145] *See* Association for Computing Machinery, ACM US Public Policy Council Comment at 6; Consumer Federation of America Comment at 5; Neal Krawetz et al. Comment at 5-6; Coalition for Cybersecurity Policy & Law Comment at 5.
[146] Microsoft Comment at 7.
[147] Jillisa Bronfman Comment at 223.
[148] Neal Krawetz et al. Comment at 12.
[149] CTIA Comment at 18 (citations omitted).

exchanged completely unencrypted information with servers.[150] Even devices that did encrypt the data traffic they sent and received were at times revealing other points of information, such as when power had been turned on or off.[151] Many commenters agreed that encryption is important in all areas of the IoT environment, including at the device level, for data in transit, and at the platform or service level. Commenters urged the government to encourage the adoption and use of the best commercial encryption implementations and security practices available.[152]

While encryption is just one of many important capabilities, it drew numerous comments. The Niskanen Center stated that strong encryption has significant economic benefits, encouraging and promoting the trust necessary for robust online commerce and finance.[153] NIST has already begun to explore the potential of "lightweight encryption" for devices with low computing power.[154]

#### ii. Privacy

Potential privacy concerns arising from the use of IoT devices were second only to cybersecurity in number of comments received. While it is clear that consumer trust is essential to the growth of IoT,[155] and that ensuring the privacy of users is a key aspect of building that trust, commenters were divided on whether IoT presents novel privacy challenges and on the appropriate response to these challenges.

It is clear that connected devices are not all equal in their relative effects on privacy. According to some commenters, industrial, agricultural, and other non-consumer facing uses of IoT generally would not likely collect information that could be considered personally identifiable information.[156] Any policy response to privacy concerns would need to avoid placing regulatory burdens on applications that pose limited potential for privacy-related harms. There is also a danger in creating too many "sector-specific" regulatory requirements. For example, the GSM Association stated that "privacy considerations that accompany IoT will affect different sectors of the economy, and conflicting, sector-specific regulations will hinder IoT development and

---

[150] Electronic Privacy Information Center Comment at 7 (citations and internal quotations omitted; emphasis original).
[151] Nick Feamster, *Who Will Secure the Internet of Things?*, Freedom to Tinker (Jan. 19, 2016), https://freedom-to-tinker.com/blog/feamster/who-will-secure-the-Internet-of-things/ (emphasis in original).
[152] *See* Computer & Communications Industry Association Comment at 10-11; ACT | The App Association Comment at 4; BSA | The Software Alliance Comment at 5.
[153] Niskanen Center Comment at 6.
[154] Draft NISTIR 8114 Report on Lightweight Cryptography (August 2016), http://csrc.nist.gov/publications/drafts/nistir-8114/nistir_8114_draft.pdf.
[155] Alain Louchez Comment at 6.
[156] GSM Association Comment at 8; Center for Data Innovation at 11. Such uses may implicate business confidential information and/or trade secret issues, *see infra* Section 3.G.iii (discussing trade secrets).

deployment."[157] Many commenters nonetheless argued for a "privacy-by-design" approach,[158] or the use of privacy enhancing technologies (PETs).[159] These techniques would typically need to be implemented before the developers determine the use for devices or components that are deployed in both consumer-facing and non-consumer facing applications.

Several commenters argued that there are no new privacy issues related to IoT,[160] that it is too early to craft regulatory responses,[161] or that current regulation is sufficient.[162] The U.S. Chamber of Commerce stated that "[w]ithout evidence of heightened privacy concerns or consumer harm, there is no reason not to allow the IoT market to mature under the frameworks that exist for protecting consumers' legitimate privacy interests."[163] These commenters primarily pointed to Federal Trade Commission enforcement of its Section 5 authority over unfair or deceptive practices, sector-specific legislation such as the Children's Online Privacy Protection Act, and the Health Insurance Portability and Accountability Act as providing the protections needed by consumers.[164] Verizon, for example, stated that "[p]olicymakers should leverage existing privacy frameworks – including the existing Federal Trade Commission regime and self-regulatory mechanism – to create a holistic policy approach to IoT-related privacy issues. Doing so will create the necessary regulatory certainty and stability to support continued investment and growth in IoT solutions."[165] These commenters are concerned about the potentially negative effect that proactive regulation would have on innovation and growth in IoT.[166]

Other commenters argued that the privacy concerns raised by IoT were either novel[167] or were different enough in scale, scope, and stakes to necessitate distinct consideration.[168] As Microsoft argued, "IoT raises unique privacy concerns. IoT will dramatically increase the number of devices facilitating the creation, collection and transmission of data. In parallel, connected devices without screens or other direct user interfaces create significant practical challenges for privacy regimes based primarily on notice and consent."[169]

---

[157] GSM Association Comment at 16.
[158] Cisco Systems Comment at 24; Jillisa Bronfman Comment at 220; Verizon Comment at 19.
[159] Electronic Privacy Information Center Comment at 11.
[160] *See* Computer & Communications Industry Association Comment at 4; Center for Data Innovation Comment at 6.
[161] *See* Niskanen Center Comment at 5; National Cable & Telecommunications Association Comment at 6; U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 3.
[162] *See* U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 11; CompTIA Comment at 5; NetChoice Comment at 2-3.
[163] U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 11.
[164] *See* Nest Labs Comment at 8-10.
[165] Verizon Comment at 17.
[166] Consumer Technology Association Comment at 16; General Motors Comment at 5.
[167] *See* Microsoft Comment at 10; Open Connectivity Foundation Comment at 6; Public Knowledge Comment at 13; ACM US Public Policy Council Comment at 6-7.
[168] *See* Symantec Comment at 1; Sysorex USA Comment at 3.
[169] Microsoft Comment at 10.

Commenters also raised the challenge of notice and consent, suggesting the need for flexibility and modernization of how consent is gained.[170] Given the vast amounts of data that IoT devices are capable of collecting, commenters also discussed the link between the privacy concerns raised by IoT and those inherent in the discussions of big data,[171] with the paramount concern being the need to combat potential discrimination, secure collected data, and promote transparent decision-making processes. Symantec states:

> The unprecedented volume of data that will be generated by connected devices will in many applications raise significant privacy issues. First and most obviously, an exponential increase in data collection brings with it a similar increase in the potential for and damage from a data breach. This data will need to be securely collected, transmitted, and stored. But the analytics that can be applied to all of this data raises different issues, as Americans are increasingly concerned with how big data is providing corporations and governments insight into their lives. As with security, the first step towards addressing these issues is transparency – people should have the opportunity to understand how data about them is being secured, just as they should know how that data is being used.[172]

Many commenters expressed significant concern about the ubiquity of data collection and the potentially sensitive or personal nature of this data. The Electronic Frontier Foundation cited a Hewlett Packard Enterprise study that "found that 90 percent of IoT devices collected at least one piece of personal information via the device, the cloud, or its mobile application."[173] At the September 2016 IoT workshop, Michelle De Mooy of the Center for Democracy and Technology stated that these concerns are intertwined with concerns about security, given that insecure data is the primary way in which user privacy is likely to be breached. Straddling the line between privacy and security concerns is the need to address data breach notification policy, which is currently a patchwork of laws and regulations.[174] Commenters also raised the need to address the problem of data ownership over the lifecycle of a consumer device.[175]

The scope of personal data collected by connected devices is potentially immense, expanding far beyond the usual concerns of traditional e-commerce. The systematic collection of personal information, habits, locations, and physical conditions over time can easily allow an entity that has not directly collected this information to infer specific details about the user or users of the

[170] Microsoft Comment at 2; Future of Privacy Forum Comment at 9; Kim L. Jones Comment at 2.
[171] Cisco Systems Comment at 26-27; Hewlett Packard Enterprise Comment at 5.
[172] Symantec Comment at 4.
[173] Electronic Frontier Foundation Comment at 2.
[174] CompTIA Comment at 5; Access Now Comment at 4.
[175] *See* Symantec Comment at 2-3; Staff of the Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning Comment at 9; Verizon Comment at 21. This also has intellectual property implications as discussed below, Part 3.B.iii.

devices, as the Federal Trade Commission pointed out in its January 2015 staff paper on IoT privacy and security.[176]

As to how these issues should be addressed, several commenters felt that the Department of Commerce, for various reasons, is not the place to develop policy in this area. For example, the Consumer Federation of America argued that "[t]he DOC is not the right place to develop U.S. privacy policy. It is not a privacy or consumer protection agency."[177] And the Niskanen Center stated that "Congress, and not a confusing hodgepodge of competing regulatory bodies, will be the primary regulator of IoT. Congress, not Executive Branch regulators, should lead on the IoT."[178] There was some support, however, for multistakeholder efforts, both facilitated by the government or in which the government acts as a participant.[179] Multistakeholder efforts call for bringing all interested stakeholders together to try to reach consensus on how to address a particular problem or issue.

One clear argument made by several of the commenters and participants in the workshop is that any approach to privacy policy from the government should be technology neutral. Hewlett Packard argued that the "overall privacy and data protection environment should be flexible enough for new technologies, and not create IoT-specific requirements."[180] Former Federal Trade Commission Commissioner Julie Brill called for technology-neutral baseline privacy legislation during the IoT workshop.[181] Through baseline privacy legislation, such as the Commerce Department's 2015 Discussion Draft based on the Consumer Privacy Bill of Rights,[182] it would be possible to address privacy concerns without regard to the type of technology used. It would also supplant the current patchwork of regulation based on information type and use.[183]

### iii. Intellectual Property

IoT technologies and uses can involve significant intellectual property issues – including copyright, patents, trade secrets, and trademarks – some of which commenters discussed and are highlighted in this section. The comments indicate that, in general, intellectual property is an important topic that deserves recognition and further consideration as IoT penetrates more

[176] Federal Trade Commission, *Internet of Things: Privacy & Security in a Connected World* (January 2015), 14, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
[177] Consumer Federation of America Comment at 7.
[178] Niskanen Center Comment at 7.
[179] *See, e.g.*, Internet Commerce Coalition Comment at 3; Southern Company Services Comment at 3.
[180] Hewlett Packard Enterprise Comment at 2.
[181] Fostering the Advancement of the Internet of Things Workshop, September 1, 2016, Transcript at https://www.ntia.doc.gov/files/ntia/publications/09012016-iot-workshop.pdf,
[182] Consumer Privacy Bill of Rights Administration Discussion Draft (2015), https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.
[183] Using a risk-based systems engineering approach to privacy could further facilitate addressing privacy concerns. See NIST research on privacy engineering at http://csrc.nist.gov/projects/privacy_engineering/index.html.

households and businesses and becomes a ubiquitous part of everyday life. Furthermore, as the comments suggest, IoT plays into ongoing intellectual property policy discussions, which address more general concerns.[184] These issues also have international policy implications.[185]

### 1. Copyright

Copyright law protects original works of authorship fixed in a tangible medium of expression by granting to authors certain exclusive rights subject to a number of exceptions and limitations.[186] The United States and many other countries also provide protection against the circumvention of technological protection measures (TPMs) designed to prevent the unauthorized use of or access to works protected by copyright.[187] Key copyright-related IoT issues involve ownership, access, and usage of data and software.

Commenters noted that there are still questions about who owns data in the IoT environment, and what may be done with it.[188] The answers will depend in part on the nature of the "data," whether it is embodied in a copyrightable compilation, and whether an exception or limitation applies.[189] Although mere "facts" (e.g., the temperature of a home) are not eligible for copyright protection, if data outputs produced by IoT devices include copyrightable sounds or images,[190] or reflect a

[184] For example, some commenters argue that patent assertion entities could stifle development of IoT. *See, e.g.*, Internet Association Comment at 9-11; Nokia Comments at 4; Public Knowledge Comments at 7; Computer & Communications Industry Association Comment at 9. The effect that litigation threats by patent assertion entities have on innovation has been a significant subject of discussion within government and the private sector for a number of years. *See*, e.g., House Energy and Commerce Committee Hearing on The Impact of Patent Assertion Entities on Innovation and the Economy, https://energycommerce.house.gov/hearings-and-votes/hearings/impact-patent-assertion-entities-innovation-and-economy.

[185] For example, TPMs and RMIs, discussed below, are part of bilateral and multilateral copyright treaties. *See* Internet Policy Task Force, *Copyright, Creativity, and Innovation in the Digital Economy*, 16-19 (2013) ("Copyright Green Paper"), http://www.uspto.gov/sites/default/files/news/publications/copyrightgreenpaper.pdf.

[186] 17 U.S.C. § 106 (listing exclusive rights of copyright holders).

[187] Section 1201 prohibits the circumvention of TPMs that effectively control access to copyrighted works ("access controls") and also prohibits trafficking in technologies or services that facilitate circumvention of TPMs that protect copyright owners' exclusive rights ("copy controls"), 17 U.S.C. § 1201(a)-(b). Section 1201 also includes certain statutory exemptions from the prohibition against circumvention, including for reverse engineering of computer programs to achieve interoperability. *See also* Copyright Green Paper, 16-18, 26-27 (describing TPMs). In addition, every three years the Librarian of Congress may issue temporary exemptions from the prohibition against circumventing TPMs. The Register of Copyrights is required to consult with the Assistant Secretary for Communications and Information at NTIA when considering what exemptions to recommend to the Librarian of Congress in a triennial rulemaking process. 17 USC Section § 1201. Exemptions granted by the Librarian under this rulemaking process last three years but may be renewed in a future proceeding. In addition to TPMs, another technological adjunct to copyright can help protect data integrity and metadata by prohibiting falsifying or removing rights management information (RMI). 17 U.S.C § 1202. *See also* Copyright Green Paper at 19 (describing RMIs).

[188] ACM U.S. Public Policy Council Comment at 4-5 (emphasizing the importance of data ownership, maintenance of data and metadata, and attribution). *See also* Consumer Federation Comment at 4; InterDigital Comment at 6 (urging Commerce department to "look ahead" to data ownership issues); Online Trust Alliance Comment at 5-6; Huawei Technologies Comment at 13.

[189] Software and data may also be subject to trade secret protection, as discussed below.

[190] Dr. Rosner Comment at 3 (noting that IoT includes low-cost webcams); SIA Comment at 1-2, noting that IoT includes video surveillance technologies. CTIA Comment at 4 (" Samsung's Family Hub refrigerator connects to the

sufficiently original selection and presentation of data,[191] then permission may be required to copy, distribute, or modify the resulting works.

Some commenters focused on how licensing terms affect the way in which consumers interact with the copyrighted software embedded in IoT devices, and argued for solutions that would enable consumers to own the copies of software embedded in the devices they purchase.[192] Other commenters stated that it is important that IoT policies do not inadvertently undermine intellectual property rights, or weaken established licensing practices.[193] One commenter pointed out copyright's important role in deterring counterfeit mobile applications by discouraging counterfeit applications that may carry malware.[194]

Some commenters focused on the impact that anti-circumvention provisions may have on access to software and data.[195] Commenters were divided on how these provisions would ultimately affect the development of IoT, and what actions the government should take as a result. For example, one commenter argued that the unrestricted ability to access and modify embedded software will threaten the reliability, safety, and usability of IoT devices.[196] Another wrote that technological protection measures inhibit security research, which they claimed further threatens consumer privacy and security.[197]

---

Internet and mobile devices so that users can order groceries, stream music, and view the contents of their fridge from anywhere"). *See also* Justin Hughes, *The Photographer's Copyright: Photograph as Art, Photograph as Database*, 25 HARV. J. LAW & TEC. 327 at 367-368, 380-81, 409 (2012) (discussing copyrightability of images produced by surveillance cameras and satellite systems).

[191] *See* U.S. Copyright Office, Cir. 14, *Copyright in Derivative Works and Compilations* (2013) ("copyright in a compilation of data extends only to the selection, coordination or arrangement of the materials or data, but not to the data itself"), http://copyright.gov/circs/circ14.pdf.

[192] Consumer Federation of America Comment at 4, 10; Consumers Union Comment at 5; Owners' Rights Initiative Comment. This issue has drawn the attention of Congress, which in October 2015 directed the Copyright Office to review the role of copyright law with respect to software-enabled consumer products. *See* http://www.copyright.gov/policy/software/. The Copyright Office issued its report December 15, 2016, and observed that:

> [T]he reach and scope of licensing practices for embedded software [is] an issue that implicates several subsidiary issues, including: the relationship of the Copyright Act to state contract law; whether, and in what circumstances, violations of the terms of software licenses would constitute copyright infringement; and confusion among consumers regarding licensing terms for embedded software. The Office's study found that, in certain circumstances, such as resale, there is only limited evidence regarding real-world restrictions. Accordingly, the Office believes that the question of ownership versus licensing, while very important, is one that can be resolved with the proper application of existing case law.

U.S. Copyright Office, Software-Enabled Consumer Products: A Report of the Register of Copyrights at iii (2016), *available at* https://www.copyright.gov/policy/software/software-full-report.pdf.

[193] BSA | The Software Alliance Comment at 6-7; ACT | The App Association Comment at 10.

[194] ACT | The App Association Comment at 10-11.

[195] *See* U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 14; Consumer Federation of America Comment at 10; Owner's Rights Comment at 2.

[196] The Software & Information Industry Association Comment at 2.

[197] Electronic Frontier Foundation Comment at 6-9.

### 2. Patents

As with any technological field, patents can be expected to play a key role in IoT development. By securing exclusive property rights for the inventors of technical advances, patents provide incentives for innovators to develop better IoT devices, manufacturing practices, and infrastructure. Several patent policy issues have the potential to impact IoT industries going forward. At present, none of these issues are unique to IoT,[198] and the USPTO and other federal agencies have been working to address a number of them.

As standards for IoT are developed in the United States and abroad, issues around standard essential patents and licensing may arise,[199] reflecting discussions currently underway in broader sectors such as information and communication technology. When private-sector standards developing organizations (SDOs) develop new consensus standards, some SDOs encourage or require participants to declare any patents they own (or pending patent applications) that would be needed to implement the standard.[200] For its part, the U.S. Government, based on longstanding policy,[201] defers to private sector SDOs to adopt approaches that meet the needs of the participating members and the industries where those standards will be used while appropriately balancing the various interests involved while fairly compensating patent owners for use of their technology.[202]

---

[198] Indeed, one commenter noted the importance of accounting for the impact of these issues on the broader economy rather than just the narrow confines of IoT. *See* Fashion Innovation Alliance Comment at 4.

[199] *See* Ericsson Comment at 2, 14; Staff of the Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning Comment at 15; ACT | The App Association Comment at 6.

[200] *See* Fed. Trade Comm'n, Prepared Statement of the Fed. Trade Comm'n before the United States Senate Comm. on the Judiciary Subcommittee on Antitrust, Competition Policy and Consumer Rights concerning Standard Essential Patent Disputes and Antitrust Law at 4-6 (July 30, 2013), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commissionconcerning-standard-essential-patent-disputes-and/130730standardessentialpatents.pdf (cited by Staff of the Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning Comment at 1, 84; ACT | The App Association Comment at 6. Most SDOs require participants to affirm whether they are willing to license any patents that are required to implement the standard, and if so, whether they are willing to license them on terms that are reasonable and non-discriminatory. Such standard essential patents are then subject to the SDO's patent licensing policy, which may require licensing the patents on fair, reasonable, and non-discriminatory (FRAND) terms to anyone using the standard.[200] In addition, several commenters suggested that governments should assist in addressing or resolving these standards-related policy differences. ACT | The App Association Comment at 6-10; Cisco Systems Comment at 15-17, 30; Ericsson Comment at 2, 14; Internet Association Comment at 9-11; Nokia Comment at 3-4, 11; Qualcomm Comment at 14-15; Microsoft Comment at 12.

[201] *See* OMB Circular A-119, https://www.whitehouse.gov/omb/circulars_a119; University of Michigan Comment at 1.

[202] In some situations, however, certain U.S. Government policymakers may have weighed in with non-binding policy statements, such as with the 2013 policy statement from the USPTO and the Department of Justice on litigation remedies for standard essential patents under FRAND commitments. https://www.uspto.gov/about/offices/ogc/Final_DOJ-PTO_Policy_Statement_on_FRAND_SEPs_1-8-13.pdf.

Patent quality is another critical issue that attracted considerable attention among stakeholders, particularly with regard to litigation.[203] The Department recognizes that clarity is important for letting industry competitors and the public know which functionality or actions are covered by a patent, when they should seek licenses, and what alternatives they can pursue. USPTO has been actively engaged on this topic with the patent community.[204] Commenters also stated that the government should address patent trolls and reduce abusive patent litigation, according to two commenters.[205]

One commenter noted the importance of providing clear eligibility for patentable subject matter in the IoT space.[206] In response to several Supreme Court cases that altered longstanding practice on eligibility, the USPTO issued guidance to patent examiners in 2014 on how to apply the Supreme Court's rulings during examination, and has been providing regular updates and teaching examples with substantial input from patent stakeholders as new court cases are decided.[207]

The Niskanen Center stated that IoT may likewise present challenges for enforceability of patents.[208] For instance, the distributed nature of IoT may raise a number of questions regarding multi-party infringement liability. Traditionally, one party must perform every element of a patent claim to be liable for infringement. However, sometimes multiple parties act together in such a way that the combined result performs the patent claims. Patent owners have limited mechanisms to enforce their patents in such situations.[209] However, these types of liability have

---

[203] Computer & Communications Industry Association Comment at 9-10; Consumer Technology Association Comment at 8; Internet Association Comment at 9-11; Public Knowledge Comment at 7-8.

[204] Recognizing the need for high-level, systemic, and operational focus on this issue, the USPTO appointed its first Deputy Commissioner for Patent Quality in 2015 and launched its "Enhanced Patent Quality Initiative" (EPQI) soon after. These efforts help to improve the clarity of the patent record (including patent scope) and increase certainty that the patent was granted in accordance with applicable statutory requirements. *See* USPTO Enhanced Patent Quality Initiative, http://www.uspto.gov/patent/initiatives/enhanced-patent-quality-initiative-0. See also, Comment of the United States Federal Trade Commission and the United States Department of Justice Before the United States Department of Commerce Patent and Trademark Office: In the Matter of Request for Comments on Enhancing Patent Quality, https://www.ftc.gov/policy/policy-actions/advocacy-filings/2015/05/comment-united-states-federal-trade-commission-united.

[205] *See* Public Knowledge Comment at 7; Annex to Nokia Comment at 2; Computer & Communications Industry Association Comment at 8. See, also, Patent Assertion Entity Activity: An FTC Study, https://www.ftc.gov/reports/patent-assertion-entity-activity-ftc-study.

[206] Niskanen Center Comment at 23.

[207] *See* USPTO 2014 Interim Guidance on Subject Matter Eligibility, http://www.uspto.gov/patent/laws-and-regulations/examination-policy/2014-interim-guidance-subject-matter-eligibility-0.

[208] *See, e.g.*, Niskanen Center Comment at 20, 22.

[209] Namely: divided infringement, where one actor directs or controls the actions of another, or when multiple actors engage in a "joint enterprise" to perform all the steps of a patent claim (*See Akamai Techs., Inc. v. Limelight Networks, Inc*., 797 F.3d 1020 (2015); active inducement, where one party induces another party to perform steps which infringe a patent claim (35 U.S.C § 271(b). *See Commil USA, LLC v. Cisco Sys*., 135 S. Ct. 1920 (2015); and contributory infringement, where one actor sells a material part of a patented invention for use by others to infringe the patent (35 U.S.C. § 271(c)).

limitations that can make it difficult to enforce certain patents, particularly since the Internet allows seamless, invisible, efficient interactions by multiple parties.

### 3. Trade Secrets

A trade secret is confidential, commercially valuable information that provides a company with a competitive advantage, such as customer lists, methods of production, marketing strategies, pricing information, and chemical formulae.[210] The type of information that could be protected as a trade secret is virtually limitless. At issue is how trade secret protection promotes IoT innovation, and how the rise of IoT impacts trade secret protection.

Trade secrets are crucial to helping our entrepreneurs and businesses start, grow, and innovate, including in the IoT space. In addition, the proliferation of devices and connectivity that makes up IoT also gives rise to trade secret vulnerabilities.[211] In relation to IoT, one commenter posited that "[p]roducts will be defined by the sophistication of their algorithms. Organizations will be valued based not just on their big data, but the algorithms that turn that data into actions and ultimately customer impact."[212] The protection and security of algorithms associated with IoT has been noted as an issue.[213] Accordingly, the protection of trade secrets is one key element to the encouragement of innovation in the IoT sphere.

Confidentiality concerns were mentioned by some commenters.[214] In business environments, data sharing without appropriate controls to protect against inadvertent release of confidential information creates additional risk that trade secrets will be exposed. Only one commenter specifically mentioned the implication of these general concerns for trade secrets, although other

---

[210] Yeh, Brian, *Protection of Trade Secrets: Overview of Current Law and Legislation*, Congressional Research Service Report No. R43714 (April 2016). http://www.fas.org/sgp/crs/secrecy/R43714.pdf.

[211] One requirement of trade secret protection is that the information must be subject to reasonable efforts to maintain secrecy. "Technologies providing greater access to information anytime and anywhere will increasingly rely on the internet, and present new challenges to companies seeking to protect information transmitted by, or contained on, mobile devices." White House, Strategy on Mitigating the Theft of US Trade Secrets (2013), https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf. The same report notes that the cultural, economic, and geopolitical shifts, in particular as employees can work and access data anywhere and at any time, not just at an office, laboratory, or factory, creates additional risks to trade secrets.

[212] Peter Sondergaard, The Internet of Things Will Give Rise to the Algorithm Economy (June 1, 2015), available at: http://blogs.gartner.com/peter-sondergaard/the-internet-of-things-will-give-rise-to-the-algorithm-economy/

[213] David Levine, What Does the Internet of Things Mean for Corporate Secrecy? Slate, (April 4, 2014), available at:http://www.slate.com/blogs/future_tense/2014/04/04/what_does_the_internet_of_things_mean_for_corporate_secrecy.html.

[214] James Andrew Lewis, *Managing Risk for the Internet of Things*, Center for Strategic and International Studies (Dec. 2015), https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151201_Lewis_ManagingRiskIoT_Web.pdf. "IoT does not change the most important problem we currently face in data and network protection – data exfiltration leading to the theft of intellectual property, business confidential information, and personal information. Most IoT devices will not store intellectual property or business confidential data."

references to proprietary, confidential, and/or sensitive information could be considered to relate to trade secrets as well.[215]

#### 4. Trademark

According to some commenters, the creation of platforms for interoperability of products and services creates opportunities for trademark owners to diversify their brand offerings but raises enforcement challenges.[216] Trademarks serve several functions for consumers and brand owners, including serving as quality indicators as well as signaling who is responsible for a substandard product.[217] Some commenters said that products falsely alleged to be compatible with a suite of proprietary branded devices or services could engender performance deficits that affect the operation of the branded products and subject the brand owner to lawsuits.[218] Use of the brand by third parties to signal interoperability presents enforcement costs as well as licensing opportunities.[219] Notably, there may be a significant role for use of certification trademarks to indicate that goods have been certified as meeting standards for device interoperability.[220] These challenges are not specific to IoT, but should be considered when deciding how best to leverage brands using these new technologies.

### iv. Free Flow of Data Across Borders

The free and open global Internet, with minimal barriers to the flow of information and services across national borders, is the lynchpin of the digital economy today.

---

[215] Niskanen Center Comment at 27 (noting that encryption can protect trade secrets).
[216] *See, e.g.*, AT&T Services Comment at 11-12 (discussing branding strategies in the context of different business models); Fashion Innovation Alliance Comment at 4 (discussing fashion brands that could be looking to integrate technology into their apparel and accessories); Annex to Comments of Internet Society at 47 ("some device manufacturers see a market advantage to creating a proprietary ecosystem of compatible IoT products…which limit interoperability to only those devices and components within the brand product line"); Comments of Security Industry Association at 3.
[217] *See, e.g.* Riley Walters Comment at 3 (observing that device security is beneficial to the IoT producer brand name).
[218] ACT | The App Association Comment at 10 (misappropriating application logic and brands to create counterfeit software applications that harm the IoT environment). Center for Strategic and International Studies Comment at 4 (manufacturer brand owners must do a risk assessment for lawsuits and liability costs if a car is shown to be unsafe because it is vulnerable to hacking).
[219] U.S law requires trademark owners to control the quality of the goods or services bearing their brand, even when the brand is licensed for use by authorized third parties.
[220] Certification trademarks may be used to certify that authorized users' goods or services meet certain standards in relation to quality, materials, or mode of manufacture (e.g., approval by Underwriters Laboratories). 15 U.S.C. §§ 1054, 1127. *See* Open Connectivity Foundation Comment at 2 (noting that it provides branding for certified IoT devices via compliance testing).

A number of commenters emphasized just how important a free and open Internet is to the future innovation and growth of IoT.[221] They stressed that cross-border information flows are critical to companies across sectors, from industrial to human resources. While some governments have created policies that limit cross-border data flows for various reasons, such policies could negatively affect the growth of certain IoT sectors by impeding the normal functioning of the devices, many of which themselves cross borders frequently (e.g., sensors on an airplane). Further, these commenters argued that these policies raise costs, especially for small and medium sized companies, which can slow economic growth.

Multiple commenters recommended that the U.S. Government continue to work with the international community to encourage the cross-border flow of data to enable IoT services and discourage forms of localization.[222] This might include work on interoperability of privacy and cybersecurity regimes and standards. Stakeholders also recommended that the U.S. Government should seek to form binding commitments with other nations to ensure the flow of information.[223]

### v. Planned Activities

The Department reaffirms its commitment to the policy approach that has made the United States the leading innovation economy. This approach is reflected in the 1997 Framework for Global Electronic Commerce,[224] and has been maintained across all subsequent Presidential administrations. It asserts that policy should generally be industry led, and that regulation, when needed, should be predictable and consistent. The Department is positioned to advance U.S. policy approaches around IoT, including those recommended in this paper. Policy related to IoT spans multiple domains from data protection and privacy issues, to infrastructure stability and security, to digital inclusion. The following issues are and will continue to be priority focus areas of the Department in the IoT domain.

#### *1. Current Initiatives*

- **International Engagements**. Government-to-government dialogues and relevant international fora are major vehicles for the Department's international engagement on IoT. Currently the Department maintains formal dialogues with numerous governments where digital economy and general information and communications technology issues are often discussed. Through stakeholder input, the Department envisions IoT and aspects

[221] *See, e.g.,* Visa comment at 7; Computer & Communications Industry Comment at 6; Trans-Atlantic Business Council Comment at 9; Information Technology Industry Council Comment at 5, Security Industry Association Comment at 4.
[222] Visa Comment at 7; Nest Labs Comment at 14-15; ACT | The APP Association Comment at 11-12.
[223] *See, e.g.,* Nest Labs Comment at 14-15; BSA | The Software Alliance Comment at 6; Computer & Communications Industry Association Comment at 6; IBM Comment at 3.
[224] The White House, The Framework for Global Electronic Commerce, (July, 1997) http://clinton4.nara.gov/WH/New/Commerce/.

thereof will continue to be raised in these engagements. In international fora, the Department engages in the work of the International Telecommunication Union and in the Internet Governance Forum (IGF) IoT dynamic coalition, among others.

- **Interagency Collaboration.** The Department will continue to work with its interagency partners to ensure the development of policy that fosters IoT innovation and protects the rights and safety of individuals.

- **Cybersecurity**. The Department will continue to bring private sector experts together with policymakers to define security principles for IoT, facilitate IoT security framework development by sector and application, and encourage the implementation of best practices and/or minimum standards.

    - **NTIA Cybersecurity Multistakeholder Process**. NTIA is convening a cybersecurity-focused multistakeholder process to address IoT security upgradability and patching.[225] The objective of this multistakeholder process is to foster a market offering more devices and systems that support security upgrades through increased consumer awareness and understanding. Enabling a thriving market for patchable IoT devices requires common definitions so that manufacturers and solution providers speak a common language.

      As the process identified, IoT has brought connectivity to business sectors that previously did not provide networked products – and some of these businesses are confronting a new requirement to deal effectively with cybersecurity threats targeting their products. The Department is assisting by working with industry and other stakeholders to document best practices for patching, vulnerability notification, and control of data retention for IoT products. In addition, the threat posed by orphan devices – devices no longer supported by their manufacturers – must also be addressed. Devices that consumers continue to use to connect to the Internet should be updated and protected even if device manufacturers discontinue them. There should be some mechanism (such as transferring the needed software keys to a designated consortium) for ensuring that devices function with the software updates needed to ensure security. Stakeholders, through NTIA's multistakeholder process, will have the opportunity to encourage providers of connected devices and services to embrace security-by-design, beginning with risk assessment as part of the design process, testing security measures before products and services launch, and using encryption to store and use sensitive information.

[225] https://www.ntia.doc.gov/files/ntia/publications/2016-22459.pdf

- **Privacy.** The Department continues to address privacy concerns in a range of contexts, from support for baseline privacy legislation that would include IoT services, to work to promote the availability of strong encryption (including in IoT devices).

- **Intellectual Property.** The Department of Commerce will continue to work to promote the positive evolution of intellectual property and its protection in the Internet's digital economy. Over the past few years, the Department has consulted extensively with stakeholders. It produced a green paper on *Copyright Policy, Creativity, Innovation, and the Digital Economy*,[226] which provided a thorough and comprehensive analysis of digital copyright policy, including issues relevant to the Internet of Things. It published a White Paper on *Remixes, First Sale, and Statutory Damages*,[227] and is conducting work as recommended in those papers, including facilitating discussions about standards and interoperability in the context of developing the online marketplace for copyrighted works.

- **Cross-Border Data Flows.** Recognizing the value of Internet openness and the free flow of information, and the risks that restrictions on Internet data flows present to innovation, economic growth, and social prosperity, the Department of Commerce has made it a top priority to ensure that information and data continue to flow freely and the Internet remains open and global. The Department has played a critical role in developing policies and initiatives that protect the free flow of information and foster a robust digital economy. For example, the Department championed the development of the *Principles for Internet Policy-Making* at the Organization for Economic Cooperation and Development (OECD).[228]

### 2. Proposed Next Steps

The Department will:

- Continue to foster an enabling environment for IoT technology to grow and thrive, allow the private sector to lead, and promote technology-neutral standards and consensus-based multistakeholder approaches to policy making at local, tribal, state, federal, and international levels on issues ranging from U.S. security and competitiveness to

[226] https://www.uspto.gov/learning-and-resources/ip-policy/copyright/green-paper-copyright-policy-creativity-and-innovation
[227] https://www.uspto.gov/learning-and-resources/ip-policy/copyright/white-paper-remixes-first-sale-and-statutory-damages
[228] Organization for Economic Cooperation and Development (OECD), Principles for Internet Policy-Making (2014), http://www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf.

cybersecurity, privacy, intellectual property, the free flow of information, digital inclusion, interoperability, and stability related to IoT.

- Identify and, where appropriate, convene multistakeholder processes on IoT policy issues based on stakeholder feedback in areas such as cybersecurity, privacy, inclusion, intellectual property, and cross-border data flows.

- Proactively engage and collaborate with other relevant agencies on IoT in order to protect the safety and rights of individuals, promote innovation, and ensure a consistent and predictable regulatory environment, such as with the Department of Homeland Security,[229] the Department of Transportation,[230] and the Food and Drug Administration,[231] among others.

- Leverage its country and industry experts and work closely with key interagency partners toward a consistent and predictable international IoT policy environment based on bottom-up, industry-led solutions.

- **Cybersecurity.**

  - Proactively support and promote cybersecurity policy for the IoT environment that encourages risk-based approaches, security by design, and the ability to fix or "patch" insecure software and devices.

  - As one of the key tools for addressing IoT cybersecurity concerns, promote the use of strong encryption in IoT services and products to address security concerns in the government's risk-based approach to the use and application of IoT technologies.

  - Collaborate with industry 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, and employing virtual private networks).

  - On December 2nd, 2016, the Presidential Commission on Enhancing National Cybersecurity presented its report to the President, which included several recommendations specific to IoT. The Department welcomes the Commission's

[229] *See* https://www.dhs.gov/securingtheIoT
[230] *See* https://www.transportation.gov/AV
[231] *See* http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

endorsement of the Department's leadership role in helping to guide cybersecurity policy, and is carefully reviewing and considering the Commission's recommendations as we move forward in our efforts to meet the nation's cybersecurity needs.

- **Privacy**. Work to address the need to protect consumer privacy in the IoT environment, and continue to support baseline privacy legislation, as well as an engineering approach to privacy.

- **Intellectual Property**. Work to promote the positive evolution of intellectual property and its protection in the digital economy.

- **Cross-Border Data Flows**. Work with its international partners toward an industry-led global marketplace that promotes innovation for IoT and supports the free flow of information, and the ability of American companies to compete fairly around the world.

## C. Promoting Standards and Technology Advancement

Numerous commenters called attention to the important role of the U.S. Government in the context of supporting the development of IoT standards, and many agreed that the U.S. Government should encourage industry-led efforts toward the adoption of voluntary, consensus-based, global standards for IoT.[232] Commenters also noted that interoperability and related standards development will be important to the success of IoT from a technical perspective, and the U.S. Government should actively support these national and international industry-led efforts.[233] A wide range of standards addressing different aspects of IoT applications – technology, connectivity, interoperability, functionality, security, usability, etc. – will be needed.

### i. Standards Development

It is the Department's position that a private-sector-led approach to standards development with appropriate government participation is fundamental to successfully developing these standards. While GS1 was concerned about the confusion that could arise from too many standards,[234] Infineon and CA Technologies discussed the way in which a diversity of industry-led standards organizations will be able to address the various aspects of the IoT environment and will likely converge.[235] Underscoring the need for a diverse set of industry-led, globally relevant IoT standards activities, the American National Standards Institute referenced the World Trade

[232] Software & Information Industry Association Comment at 12; Symantec Comment at 4-5; Visa Comment at 7; Cisco Systems Comment at 30; Consumer Technology Association Comment at 8-9.
[233] *See* AIM Comment at 8; AIM North America Comment at 8; Alliance of Automobile Manufacturers at 6; Local Innovation Comment at 7; National Association of Realtors Comment at 2.
[234] *See*; GS1 US Comment at 14-15.
[235] *See* CA Technologies Comment at 2; Infineon Technologies Americans Comment at 5.

Organization Technical Barriers to Trade Agreement Committee Decision, which states that the global relevance of a standard is determined by how it was developed, not by where it was developed.[236] Given the systems engineering nature of IoT applications, it is not surprising that different standards and specifications address different needs in each layer of the system stack. A range of standards organizations are already enabling standards development that is private-sector led, open, voluntary, consensus-based, and nimble.[237] New organizations are being established to meet IoT standards and specification needs as applications evolve for IoT technology.

Industry, with active participation from government experts as needed, is ideally positioned to lead the development of technological standards and solutions to address global IoT environment opportunities and challenges. The American National Standards Institute strongly advocated for the multiple-path approach to IoT standardization. Under the multiple-path approach, the relevance and utility of a standard is not linked to the organization that developed it, and multiple or competing standards can be used as solutions to meet given requirements. It added that this will help sustain a level playing field for standards organizations in which standards have been developed in a balanced, open, consensus-based process.[238] The Consumer Technology Association suggested that an emphasis on commercial solutions and market-developed voluntary standards would foster faster adoption of IoT and increased innovation.[239]

Commenters pointed to the fact that governments can work as both facilitator and convener to identify standards needs and priorities, and in such instances, they should ensure full industry participation in these processes.[240] The Information Technology Industry Council urged the Department to strongly encourage governments to participate in industry-led standardization activities, but governments should not take the lead or direct development of standards.[241] In

---

[236] American National Standards Institute Comment at 2; National Association of Manufacturers Comment at 2.
[237] *See* http://www.consortiuminfo.org/links/linksall.php for a full list of information and communication technology standards organizations.
[238] American National Standards Institute Comment at 2.
[239] Consumer Technology Association Comment at 9 (citations omitted).
[240] *See* Software & Information Industry Association Comment at 6; L Jean Camp, Ryan Henry, Steven Meyers, Gianpaolo Russo Comment at 5; AT&T Services Comment at 35-36. The Department follows guidance laid out in the Memorandum on Principles for Federal Engagement in Standards Activities to Address National Priorities (M-12-08), jointly issued by the Executive Office of the President's Office of Management and Budget, Office of the U.S. Trade Representative, and Office of Science and Technology Policy. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-08.pdf.
[241] *See*, for a fuller description of the current USG approach to standards development, https://www.whitehouse.gov/omb/inforeg_infopoltech; https://www.whitehouse.gov/blog/2014/02/14/updating-guidance-use-voluntary-consensus-standards-promote-smarter-regulation-col-0; This approach is set out in OMB Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities (revised January, 2016). *See also*, OMB Memorandum M-12-08 (January, 2016), https://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-08_1.pdf, which states: "The vibrancy and effectiveness of the U.S. standards system in enabling innovation depend on continued private-sector leadership and engagement. Most standards developed and used in U.S. markets are created with little or no government involvement. This approach – reliance on private sector leadership, supplemented by federal government

cases where multilateral organizations wish to lead standards efforts, the Information Technology Industry Council suggested those organizations should allow full industry participation, and should avoid engaging in standardization activities that may duplicate, or even conflict with, global industry-led IoT standards.[242]

Due to the vast and expansive nature of the technologies underpinning IoT, no single standards developing organization has the resources or the expertise to develop all of the standards that will be needed. Commenters have called attention to the important role the U.S. Government could play in advocating for the development and use of international standards and specifications developed in industry-led efforts that are voluntary, consensus-based, and open to participation by interested stakeholders.[243]

Commenters specifically detailed the U.S. Government's ongoing role in United Nations agencies such as the International Telecommunication Union's Standardization Sector (ITU-T) and the World Intellectual Property Organization, where IoT activities are currently underway.[244] Various commenters noted concerns about the ITU-T.[245] Comments covered concerns with proposed scope and the potential for duplication of work underway in other standards organizations.[246] Commenters urged the U.S. Government to encourage international partners to support the development and use of international standards to the extent practicable and advocate against standards that are developed in processes that are not open to all interested stakeholders or that do not treat all stakeholders in a similar manner.[247] Concern was also expressed about standards development activities that do not have strong industry support or participation.[248] To prevent possible market access barriers, commenters generally agree that the U.S. Government

---

contributions to discrete standardization processes … – remains the primary strategy for government engagement in standards development. Consistent with the Administration's commitment to openness, transparency, and multi-stakeholder engagement, all standards activities should involve the private sector."

[242]Information Technology Industry Council Comment at 12 (citations omitted).

[243] Semiconductor Industry Association Comment at 5; Trans-Atlantic Business Council Comment at 10; Telecommunications Industry Association Comment at 2. This approach is consistent with the longstanding policies of the U.S. Government, which has articulated the importance of the decision contained in Annex 2 of the Decisions and Recommendations adopted by the WTO's TBT. The TBT Committee stated that principles and procedures for transparency, openness, impartiality, consensus, effectiveness and relevance, coherence and addressing the concerns of developing countries should be observed when international standards are being developed (G/TBT/1 Rev 12, 2015). TBT Committee, G/TBT/1/Rev.12 (2015), https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=129845,121467,101299,87898,63749,11467,12694,21998,31618,23495&CurrentCatalogueIdIndex=0&FullTextHash.

[244] GSM Association Comment at 20; Niskanen Center Comment at 20-21, 34; Ericsson Comment at 11.

[245] *See* Internet Society Comment at 16; 5G Americas Comment at 9; U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 18.

[246] Verizon Comment at 17, 24; U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 18.

[247] AIM Comment at 3; U.S. Council for International Business Comment at 2-3.

[248] 5G Americas Comment at 9. GSM Association Comment at 20.

should continue to press adoption of standards that are developed in an open, globally relevant manner.[249]

Market forces will undoubtedly shape IoT development and innovation. The Department of Commerce agrees with commenters that an industry-led, bottom-up, consensus-based approach to standards development is necessary to realize the benefits of the technology.

### ii. Planned Activities

The U.S. Government fosters an industry driven, private sector-led consensus-based approach to standards development. In some other countries or regions, however, governments can have a distorting effect by identifying and directing standardization priorities and funding the development of those priorities to favor their own entities, or where participation and/or decision making in standards organizations is not open to all interested stakeholders, approaches developed may not effectively address the needs of IoT. The rationale provided by governments for active and often interventionist roles in standards development is that it is required by national/regional laws or policies, to support government policies and legislation, or to foster the development of standards to meet requirements that are unique to that country or region. It is clear from commenters that technical standards need to be developed and maintained in order to ensure that IoT reaches its full potential. This will require all parties to work within voluntary consensus standards development bodies to ensure the development, deployment, and interoperability of the IoT environment. The Department will continue to support IoT standards development that is bottom up and private-sector led. Technology development in the form of hardware and software advancement and new applications and devices will also be critical to IoT growth and adoption.

#### *1. Current Initiatives*

- **The Cyber-Physical Systems Public Working Group** (CPS PWG), formed by NIST in 2014, brings together experts to help define and shape key aspects of cyber-physical systems to accelerate their development and implementation within multiple sectors of our economy. Through its five subgroups, the CPS PWG has prepared a Cyber-Physical Systems Framework.

- **The Global City Teams Challenge** is a NIST initiative to advance the deployment of IoT technologies within a smart city environment. Nearly 100 teams or "action clusters" are pursuing projects related to energy, transportation, public safety, and other key sectors.

[249] American National Standards Institute Comment at 2; ARM Comment at 12; BSA | The Software Alliance Comment at 2; Microsoft Comment at 1.

- **The International Technical Working Group on IoT-Enabled Smart Cities Framework** is a NIST effort comparing and distilling current architectural efforts among the many smart city projects currently underway around the world. The goal is to produce a consensus framework document of common architectural features that will help cities employ interoperable and scalable smart city solutions that will meet the needs of their communities.

- **CPS Research and Standards Development** are carried out in multiple NIST laboratories, including programs in advanced manufacturing, cybersecurity, buildings and structures, disaster resilience, and smart grid.

- **NTIA Monitoring of ITU-T Study Group 20.** NTIA will continue to monitor the activities of the Standardization (ITU-T) Study Group 20 on the Internet of Things and Smart Cities and communities (SC&C), which is studying IoT, its applications, and big data aspects of IoT Smart Cities.

- **Cybersecurity for IoT Program** The NIST Cybersecurity for IoT Program focuses on fundamental and applied research and the transfer of these to industry to enable technology advancement and innovation. NIST has active ongoing work in fundamental research, including standards and guidance, that address security (e.g., lightweight encryption; RFID and Bluetooth security; systems security engineering; industrial control systems security; and blockchain). Applied research for IoT security at NIST focuses on work to address market-focused application of research through partnering with industry verticals such as Health Information Technology, Vehicle/Transportation, Smart Home and Manufacturing. For example, the National Cybersecurity Center of Excellence (NCCoE) engineers are working with the health care community to address wireless infusion pump security in hospital environments and publish best practices to address commonly found security risks.

### *2. Proposed Next Steps*

The Department will:

- Monitor IoT related technology developments and applications and contribute to research and development involving those technologies.

- Advocate for industry-led, consensus-based, international standards for IoT technologies and applications in its bilateral and multilateral engagements.

- Actively participate in, and contribute to, the development of technical standards for IoT.

## D. Encouraging Markets

Beyond the research and development work done by NTIA, NIST, and other government agencies, the U.S. Government as a whole, and the Department of Commerce in particular, can help to encourage the development and growth of the market for IoT devices by being a leading consumer and adopter of IoT; help to address the workforce issues that will arise due to the deployment of IoT; and help to better understand, plan for, and respond to IoT through quantification and measurement.

### i. Public-Private Partnerships and Government Procurement

The U.S. Government is relevant not only as a potential policy maker and regulator, but also as an enabler and adopter. The Public sector can be a leading adopter of emerging technologies, helping to promote compatible regulatory regimes on security, privacy, and intellectual property, as well as transparent and predictable market access regimes. As the Center for Data Innovation commented, "the federal government can reduce the perceived risk of the technology that limits investment and adoption by the private sector and state and local governments. The government should actively pursue opportunities to deploy connected technologies to improve mission delivery, as well as comprehensively examine opportunities to transform agency operations around the potential of the Internet of Things and the data it generates."[250]

In addition, the Department plays an important role in educating foreign markets about the benefits of new and emerging technologies, and in promoting U.S. technologies in those arenas. The Department also measures market changes, educates policymakers and the public about market developments, and designs and promotes policies that prepare the U.S. economy for changes that emerging technologies may bring.

### ii. Workforce Issues: Education, Training, and Civil Liberties

Over the past two decades, the Internet has spurred incredible innovation in the U.S. economy and positioned the United States as a global leader in information technology, according to the Consumer Technology Association.[251] In particular, advances in IoT are enabling efficiency in the home and workplace, and delivering more narrowly tailored services to businesses and consumers. As Ligado Networks suggested: "US manufacturers will gain a significant competitive advantage by lowering costs and enabling production efficiencies, reinvigorating domestic production, and allowing US manufacturers to compete with low-cost manufacturers globally."[252] BSA | The Software Alliance noted that by 2020, there will be more than 50 billion

[250] *Id*. and Cisco Systems Comment at 10.
[251] *See* Consumer Technology Association Comment at 5.
[252] Ligado Networks Comment at 17.

connected devices relied upon by consumers, governments, and businesses,[253] and Ligado said that, by 2025, 80 percent of U.S. manufacturers will have implemented IoT technologies.[254]

However, the growth potential could stall without adequate preparation for an economy that relies more heavily on IoT. The State of Illinois commented that IoT will allow for U.S. manufacturers and businesses to increase automation and efficiencies, perhaps increasing the pressure to eliminate jobs that may no longer be needed as the technology may be more cost-effective.[255] In order for the United States to take full advantage of developments in an IoT economy, the U.S. Chamber of Commerce Center for Advanced Technology and Innovation suggests that the Department will need to prepare U.S. workers for a shift in workforce education and training needs.[256] Recommendations from commenters include:

- Education incentives (e.g., grants, scholarships) for key IoT-related professions such as data science and engineering.[257]
- Partnerships with universities to develop specialized curricula.[258]
- Training opportunities (e.g., seminars, workshops) for businesses adopting IoT technologies.[259]

Education and training are not the only challenges of a workforce conversion in light of IoT adoption. The American Bar Association believes the Department will need to pay attention to individual worker rights and liberties, as some uses of IoT could be invasive (e.g., employee monitoring) or discriminatory.[260] Scott R. Peppet of the University of Colorado School of Law commented that an employer could use data from an employee's Fitbit device to infer employee behavior.[261] This is problematic for several reasons, including that the device could be giving the wrong location. The Federal Trade Commission described in their comments how data on employee commuter distance could, depending on how it is used, violate the equal-employment-opportunity standards.[262] These examples reveal the chasm between the data analysis potential that serves both as a driver for efficiency and innovation and as a potential harbinger for civil rights abuses if not managed to account for these issues. If these changes are not properly addressed, as the State of Illinois commented, low-skilled laborers who may not receive the

[253] BSA | The Software Alliance Comment at 4.
[254] Ligado Networks Comment at 17.
[255] *See* State of Illinois Comment at 22; Motorola Solutions Comment at 4.
[256] *See* U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 17.
[257] *See* Booz Allen Hamilton Comment at 15.
[258] *See* Cisco Systems Comment at 29.
[259] *See Id*.
[260] *See* American Bar Association Section of Science and Technology Law Comment at 7.
[261] *See* Scott R. Peppet Comment at 29.
[262] *See* Staff of the Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning Comment at 9.

training and resources needed to stay relevant could find themselves at a disadvantage compared with other workers.[263]

### iii. Quantifying the IoT Sector

The Request for Comment asked several questions regarding whether, and how, the government should measure the IoT sector and its economic impact. Most commenters did not address these questions, and those who did suggested that quantification of IoT was not a high priority. Several commenters even advised against government measuring IoT at this stage. The Competitive Carriers Association recommended not "formulating premature quantification and metrics"[264] while the GSM Association suggested that the private sector is best-positioned to quantify the benefits of IoT, such as cost savings, productivity growth, and other efficiencies.[265] In contrast, the Center for Data Innovation suggested that government should make measuring IoT a priority, citing the importance of understanding the role of IoT in the industrial value chain, as well as which sectors are adopting IoT rapidly and which are not.[266] In particular, they recommended focusing on understanding the value generated by IoT devices as components of the industrial value chain and measuring IoT as part of the broader technology spending."[267] With respect to analytic techniques, Booz Allen Hamilton suggested that "IoT lends itself to traditional measures and forecasts of economic impact," combining broad estimates of economic activity tied to IoT and more targeted impact assessment. Given the complexities of IoT, however, Booz Allen noted that the targeted impact assessment approach would require careful differentiation of which components should be considered IoT and which should not.[268] Additionally, the commenter also suggests that "IoT may necessitate development of new cross-industry or cross-system measures," in which case the government should leverage its "cross-industry working groups or stakeholder listening discussions to gather information" about what and how to measure.[269] The Department will take these comments into consideration in its future information-gathering efforts regarding IoT.

### iv. Planned Activities

It is clear from commenters that the government can play an important role in fostering the development of IoT through government application, procurement, and international engagements.[270] The Department is already actively engaged in promoting innovation both

[263] *See* State of Illinois Comment at 22.
[264] *See* Competitive Carriers Association Comment at 24.
[265] *See* GSM Association Comments at 14.
[266] *See* Center for Data Innovation Comment 16-17.
[267] *Id.*
[268] *See* Booz Allen Hamilton Comment at 17.
[269] *Id.*
[270] Association for Computing Machinery U.S. Policy Council Comment at 7; Nest Labs Comment at 15; 5G Americas Comment at 9-12; ACT | The App Association Comment at 11.

within the Department, domestically, and abroad, and will continue to be a champion of emerging technologies and the digital economy, as described in the examples below.

### *1. Current Initiatives*

- **Census Enterprise Data Collection and Processing Initiative (CEDCaP).** The CEDCaP aims to unify more than 100 systems used in the 2010 census to a single platform by the 2020 census, allowing shared data collection and processing across all censuses and surveys. One part of this initiative is incorporation of IoT technology into the work of the 20,000 census field workers.[271]

- **Skills for Business Initiative.** The Department has committed to use all of its pertinent assets to strengthen regional economies by supporting employer-led partnerships to address talent pipeline challenges, including within emerging technologies such as IoT.

- **Census Bureau Research on 1099 Form.** Recent advances in technology have changed how workers and employers interact in the 21st century labor market, and it is essential that our measures of employment and earnings evolve in order to remain accurate and relevant. To that end, the Census Bureau is conducting new research using IRS tax records from the "1099 form" for services performed by independent contractors as well as the use of contract workers at U.S. employer firms. These projects will inform how our labor market is evolving already and how our statistical system should evolve in response to a labor market that is dynamic due to developments such as the emergence of IoT.

- **The National Oceanic and Atmospheric Administration's (NOAA) Whale Alert.** NOAA incorporates a variety of IoT sensors, provided in collaboration with many of its partners, to collect and distribute information on Earth's environment, from local weather data to the location of whales and other marine mammals. As an example of a particular IoT data collection application, NOAA is collecting user-contributed information on Earth's magnetic field via a free smartphone app that provides users the option to share data with the agency from a phone's internal digital compass. The smartphone compass data is then used by NOAA scientists to construct new, more detailed models of the Earth's varying magnetic field, which are in turn used for a wide variety of precision navigation applications in industry. This high resolution description of the magnetic field in complex areas such as cities and other developed areas would have otherwise been costly and difficult to achieve.[272]

[271] Grayson Ullman, Census Bureau aims to save $5.2B with IoT and mobile tech, Fed Scoop (Nov. 4, 2015), http://fedscoop.com/census-bureau-to-save-2-5-billion-with-iot-tech.
[272] Larry O'Hanlon, Smartphone app seeks to make navigation safer, EOS (Jan. 6, 2015), https://eos.org/articles/smartphone-app-seeks-make-navigation-safer.

- **Commerce Data Service.** This team of designers, developers, software engineers, and data scientists works to transform raw data from the 12 bureaus, including data collected through connected devices, into insights, products, and applications to empower data-driven decision making.

- **Digital Trade Officers, Intellectual Property Attachés, and Standards Attachés**. To respond to the benefits and challenges associated with the digital economy, including IoT, the Department launched a pilot program in March 2016 for Digital Trade Officers to facilitate U.S. private sector involvement in the global digital economy and to help U.S. companies reach markets worldwide. This initiative and its pilot (launched in Brazil, China, Japan, India, the European Union, and in the Association of Southeast Asian Nations [ASEAN] region) are led by the Department's International Trade Administration (ITA), working with bureaus across the Department, in collaboration with the State Department and industry stakeholders. The Digital Trade Officers advance commercial diplomacy by driving policy advocacy on technology issues, ensure linkages between trade policy and trade promotion efforts, and provide front-line assistance for U.S. small and medium enterprises to take advantage of the robust e-commerce channels. ITA also has Standards Attachés in four U.S. embassies and consulates who are able to proactively monitor and work to address standards issues that have potential trade implications for U.S. industry and businesses.

  In addition, USPTO Intellectual Property Attachés aid U.S. embassies, consulates, and international missions.[273] The attachés advocate improving intellectual property policies, laws and regulations abroad, and provide information to help U.S. stakeholders entering foreign markets or conducting business abroad, including on IoT-related issues.

### *2. Proposed Next Steps*

The Department will:

- Continue to work toward fulfilling the missions of its various bureaus with greater impact and efficiency by leveraging emerging technologies such as IoT.

- Inform and influence government practices (purchasing and otherwise) in the use of emerging technologies such as IoT in a way that maximizes efficiency and the public good while protecting the security and privacy of individuals, which will help promote a market for devices that are consistent with these practices.

[273] *See* Intellectual Property Attaché Program, U.S. Patent and Trademark Office website, https://www.uspto.gov/learning-and-resources/ip-policy/intellectual-property-rights-ipr-attach-program/intellectual.

- Leverage its role as an IoT consumer to promote a market for secure IoT technologies and the supply chains supporting those technologies.

- Play an active role in 21st century skills development by inserting the business perspective into federal workforce policy making to support creation of quality career paths for workers, particularly in areas of emerging technologies such as IoT, to meet employer demand.

- Incorporate the Internet of Things into current education and awareness programs, such as the USPTO's Global Intellectual Property Academy, which provides intellectual property training in the United States and around the world.

- Explore developing metrics to better understand the role of IoT in the industrial value chain and its contributions to GDP, exports, and other economic measures. The Department will establish a definition for the digital economy and develop estimates of the domestic output, value added, and employment associated with the digital economy.

- Conduct research to improve the measurement of information and communications technology-enabled goods and services (including IoT) in order to improve the estimate of GDP, particularly as it relates to the digital economy, and productivity.

## 5. Conclusion

The Department recognizes the exciting promise of IoT in benefiting the lives of individuals, the economy, and society. This potential flows from a broad range of positive potential results, including increased efficiencies in industrial supply chains and systems; better use of resources through investment in Smart Cities and infrastructure; improved health and safety; and new, innovative consumer devices and possibly even as-yet-unimagined industries. Realizing these benefits will not be without obstacles, as the necessary infrastructure and policies must be in place to foster its growth while protecting individuals and society. The challenges of IoT are not all new, but in many instances are rather extensions of existing information and communication technology conversations. At the same time, IoT and its concurrent challenges are qualitatively different in that IoT increases the scale, scope, and stakes of these issues.

The approach described above is an articulation and strong affirmation of the decades-old U.S. Government approach to innovation and emerging technology, tailored to address the unique opportunities and challenges presented by IoT through the tools available to the Department of Commerce. Consistent with the values laid out in the Department's approach, our continued engagement with stakeholders is critical to crafting policy that will help to foster an innovative

IoT environment that protects individuals. Accordingly, the Department is seeking further comment on the issues discussed in this report, and intends for the comments responding to this green paper to contribute to the Department's domestic policy efforts and international engagement related to IoT.

## Appendix A: Proposed Next Steps

In addition to continuing the Department's ongoing work on IoT, this green paper identifies the following next steps for the Department and its bureaus, budget and resources permitting. The Department will:

### Enabling Infrastructure Availability and Access

- Coordinate with the private sector, as well as federal, state, and local government partners, to ensure the infrastructure to support IoT continues to expand, that access to infrastructure is inclusive and affordable, and that the infrastructure remains innovative, open, secure, interoperable, and stable. This includes promoting adoption and usage to encourage deployment and investment, and engaging in technical assistance and research and development.

- Continue to innovate in spectrum management to increase access to spectrum that will help facilitate IoT growth and advancement. NTIA, through its Office of Spectrum Management, will collaborate with stakeholders, including its spectrum-related interagency (Policy and Plans Steering Group and Interdepartmental Radio Advisory Committee) and external advisory bodies (Commerce Spectrum Management Advisory Committee), to assess the spectrum implications of the diverse IoT applications that currently or in the future may be delivered through a number of technologies operating in various spectrum bands.

- Expand its digital inclusion efforts to include an emphasis on IoT adoption and availability.

- Continue to encourage the adoption of IPv6 by fostering multistakeholder collaboration and dialogue, and provide a platform for discussion on issues such as mobile IPv6 routing, security in dual-stack environments, and privacy implications of IPv6.

- Collect data and conduct analysis on the usage and growth of IoT devices through its Digital Nation data collection in order to better inform industry and policy makers.

### Crafting Balanced Policy and Building Coalitions

- Continue to foster an enabling environment for IoT technology to grow and thrive, allow the private sector to lead, and promote technology-neutral standards and consensus-based multistakeholder approaches to policy making at local, tribal, state, federal, and international levels on issues ranging from U.S. security and competitiveness to cybersecurity, privacy, intellectual property, the free flow of information, digital inclusion, interoperability, and stability related to IoT.

- Identify and, where appropriate, convene multistakeholder processes on IoT policy issues based on stakeholder feedback in areas such as cybersecurity, privacy, inclusion, intellectual property, and cross-border data flows.

- Proactively engage and collaborate with other relevant agencies on IoT in order to protect the safety and rights of individuals, promote innovation, and ensure a consistent and predictable regulatory environment, such as with the Department of Homeland Security,[274] the Department of Transportation,[275] and the Food and Drug Administration,[276] among others.

- Leverage its country and industry experts and work closely with key interagency partners toward a consistent and predictable international IoT policy environment based on bottom-up, industry-led solutions.

- **Cybersecurity.**

  - Proactively support and promote cybersecurity policy for the IoT environment that encourages risk-based approaches, security by design, and the ability to fix or "patch" insecure software and devices.

  - As one of the key tools for addressing IoT cybersecurity concerns, promote the use of strong encryption in IoT services and products to address security concerns in the government's risk-based approach to the use and application of IoT technologies.

  - Collaborate with industry 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, and employing virtual private networks).

  - On December 2nd, 2016, the Presidential Commission on Enhancing National Cybersecurity presented its report to the President, which included several recommendations specific to IoT. The Department welcomes the Commission's endorsement of the Department's leadership role in helping to guide cybersecurity policy, and is carefully reviewing and considering the Commission's recommendations as we move forward in our efforts to meet the nation's cybersecurity needs.

[274] *See* https://www.dhs.gov/securingtheIoT
[275] *See* https://www.transportation.gov/AV
[276] *See* http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

- **Privacy**. Work to address the need to protect consumer privacy in the IoT environment, and continue to support baseline privacy legislation, as well as an engineering approach to privacy.

- **Intellectual Property**. Work to promote the positive evolution of intellectual property and its protection in the digital economy.

- **Cross-Border Data Flows**. Work with its international partners toward an industry-led global marketplace that promotes innovation for IoT and supports the free flow of information, and the ability of American companies to compete fairly around the world.

### Promoting Standards and Technology Advancement

- Monitor IoT-related technology developments and applications and contribute to research and development involving those technologies.

- Advocate for industry-led, consensus-based, international standards for IoT technologies and applications in its bilateral and multilateral engagements.

- Actively participate in, and contribute to, the development of technical standards for IoT.

### Encouraging Markets

- Continue to work toward fulfilling the missions of its various bureaus with greater impact and efficiency by leveraging emerging technologies such as IoT.

- Inform and influence government practices (purchasing and otherwise) in the use of emerging technologies such as IoT in a way that maximizes efficiency and the public good while protecting the security and privacy of individuals, which will help promote a market for devices that are consistent with these practices.

- Leverage its role as an IoT consumer to promote a market for secure IoT technologies and the supply chains supporting those technologies.

- Play an active role in 21st century skills development by inserting the business perspective into federal workforce policy making to support creation of quality career paths for workers, particularly in areas of emerging technologies such as IoT, to meet employer demand.

- Incorporate the Internet of Things into current education and awareness programs, such as USPTO's Global Intellectual Property Academy, which provides intellectual property training in the United States and around the world.

- Explore developing metrics to better understand the role of IoT in the industrial value chain and its contributions to GDP, exports, and other economic measures. The Department will establish a definition for the digital economy and develop estimates of the domestic output, value added, and employment associated with the digital economy.

- Conduct research to improve the measurement of information and communications technology-enabled goods and services (including IoT) in order to improve the estimate of GDP, particularly as it relates to the digital economy and productivity.

## Appendix B: Questions for Further Discussion

This green paper is part of the Department's ongoing engagement with the public, industry, and our sister agencies on IoT. Shortly after the release of this paper, the Department will issue an additional Request for Comment presenting the following questions for further discussion and consideration by policymakers:

1) Is our discussion of IoT presented in the green paper regarding the challenges, benefits, and potential role of government accurate and/or complete? Are there issues that we missed, or that we need to reconsider?
2) Is the approach for Departmental action to advance the Internet of Things comprehensive in the areas of engagement? Where does the approach need improvement?
3) Are there specific tasks that the Department should engage in that are not covered by the approach?
4) What should the next steps be for the Department in fostering the advancement of IoT?

## Appendix C: Acknowledgements, Workshop Panelists, and Request for Comment Respondents

The Digital Economy Leadership Team and Internet Policy Task Force extends its thanks to all of the individuals and organizations who participated in our public Workshop on Fostering the Advancement of the Internet of Things, and those who submitted written comments to the Notice of Inquiry that served as the basis for this report.

### *Workshop Panelists (as identified in the Workshop agenda):*

Bridget Karlin –Intel IoT Strategy and Integrated Products

Dean Garfield –Information Technology Industry Council (ITI)

Hilary Cain –Technology and Innovation Policy, Toyota

John Godfrey –Samsung Electronics America

Sterling Rooke –X8

Kenneth Tobin – Electrical & Electronics Systems Research Division, Energy & Environmental Sciences Directorate, Oak Ridge National Laboratory

Dan Caprio – The Providence Group

Michelle De Mooy – Center for Democracy and Technology (CDT)

Harley Geiger – Rapid 7

John Kuzin – Qualcomm

Craig Spiezle – Online Trust Alliance

Kenya Wiley – Fashion Innovation Alliance

Hardik Bhatt – Department of Innovation & Technology, State of Illinois

Julie Brill – Hogan Lovells

Leonard Cali – Global Public Policy, AT&T

Cameron F. Kerry – Sidley Austin

### *Request for Comment Respondents*

5G Americas

ABA Section of Science & Technology Law
Access Now
ACM U.S. Public Policy Council
ACT | The App Association
AIM, Inc.
AIM North America
Alliance of Automobile Manufacturers
American National Standards Institute
Anonymous
Application Developers Alliance
ARM
Association of Global Automakers, Inc.
AT&T Services, Inc.
Booz Allen Hamilton Inc.
Bronfman, Jillisa
BSA | The Software Alliance
Bugcrowd
CA Technologies
Camp, L Jean, Henry, Ryan, Myers, Steven, Russo, Gianpaolo
Center for Data Innovation
Center for Strategic and International Studies
Cisco Systems, Inc.
Coalition for Cybersecurity Policy & Law
Common Sense Kids Action
Competitive Carriers Association
CompTIA
Computer & Communications Industry Association
Consumer Federation of America
Consumer Technology Association
Consumers Union
CTIA
Deere & Company
Duckduckgo
Direct Marketing Association
Edison Electric Institute
Electronic Frontier Foundation
Electronic Privacy Information Center
Ericsson
Family Online Safety Institute
Farance, Frank (1)
Farance, Frank (2)

Farhat, Karim
Fashion Innovation Alliance
Future of Privacy Forum
Gallagher, John
General Motors, LLC
Georgia Institute of Technology, Center for Advanced Communications Policy and Rehabilitation Engineering Research Center for Wireless Technologies
GS1 US
GSM Association
Hewlett Packard Enterprise
Huawei Technologies, Inc.
Hughes Network Systems, LLC
IBM
IEEE-USA
Infineon Technologies Americas Corp.
Inmarsat, Inc.
InterDigital, Inc.
Internet Architecture Board
Internet Association
Internet Commerce Coalition
Internet Society
IoT Policy Network
ITI
James, Gilbert
Jones, Kim L.
Krawetz, Neal ; Schultz, Eric; Kaminsky, Valerie; Tucker, Bill; et al
Kurz, Jack
Lanting, Dr Cees J.M.
Larry, J. Christopher
LeFlore, Fannie
Ligado Networks
Local Innovation and Skill Cluster Anchor Network Project, Safe and Healthy Communities Project/All Communities Agenda, Internet Public Trust
Louchez, Alain
Manwaring, Kayleen
Marcus, Dr Robert
Microsoft Corporation
Milne, Claire
Mobile Future
Motorola Solutions, Inc
monica2

National Association of Manufacturers
National Association of REALTORS
National Cable & Telecommunications Association
National Emergency Number Association, National Association of State 9-1-1 Administrators
Nest Labs, Inc.
NetChoice
Niskanen Center
Nokia
Online Trust Alliance
Open Connectivity Foundation
Owners' Rights Initiative
Peppet, Scott R.
Plessel, Todd
Pratt, Steve
Providence Group
Public Knowledge
Qualcomm Incorporated
Raff, John
Rapid7
Renkis, Martin A.
Rosner, Dr. Gilad L.
Samsung
Samsung (2)
Samsung (3)
Satellite Industry Association
Schoepf, Walter H.
Secure ID Coalition
Security Industry Association
Semiconductor Industry Association
Senators Schatz, Fischer, Booker, and Ayotte
Silver Spring Networks
Software & Information Industry Association
Southern Company Services, Inc.
Spiess, Tony
Staff of the Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning
State of Illinois
Symantec
Sysorex USA
T-Mobile USA, Inc.
Telecommunications Industry Association

Thierer, Adam
Tim - The "Oldcommguy(tm)"
Trans-Atlantic Business Council
Trib1
University Corporation for Advanced Internet Development (d/b/a "Internet2")
University of Michigan
U.S. Chamber of Commerce Center for Advanced Technology and Innovation
U.S. Council for International Business
United States Telecom Association
Verizon
Visa Inc.
Vodafone US Inc. (12.7 MB)
Walters, Riley
Wi-Fi Alliance
Withrow, Scott C.
Wireless Infrastructure Association
Zebra Technologies Corporation