National Telecommunications and Information Administration

The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

RESPONSE TO REQUEST FOR COMMENT

June 2, 2016

Submitted by:

Booz Allen Hamilton Inc.
8283 Greensboro Drive
McLean, VA 22102

Point of Contact:
Nyla Beth Gawel
901 15th Street, NW
Suite 400
Washington, DC 20005
Email: gawel_nyla@bah.com
Phone: 202-898-3401

Booz | Allen | Hamilton

Booz | Allen | Hamilton

Booz Allen Hamilton Inc.
8283 Greensboro Drive
McLean, VA 22102

Tel 1 703 902 5000
www.boozallen.com

June 2, 2016

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Attn: IOT RFC 2016
Washington, DC 20230.

Subject: Response to: The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

Dear Mr. Hall:

Booz Allen Hamilton Inc. (Booz Allen) is pleased to submit this response to the Request for Comment entitled The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things.

Booz Allen has built an integrated and multi-functional Internet of Things practice, and we are ready and eager to help the Department of Commerce and other Federal agencies prepare for their involvement in accelerating development, adoption, and assessment of the Internet of Things. If you have any questions about our response, please contact me at gawel_nyla@bah.com.

Sincerely,

Nyla Beth Gawel
Principal

BOOZ ALLEN HAMILTON INC.

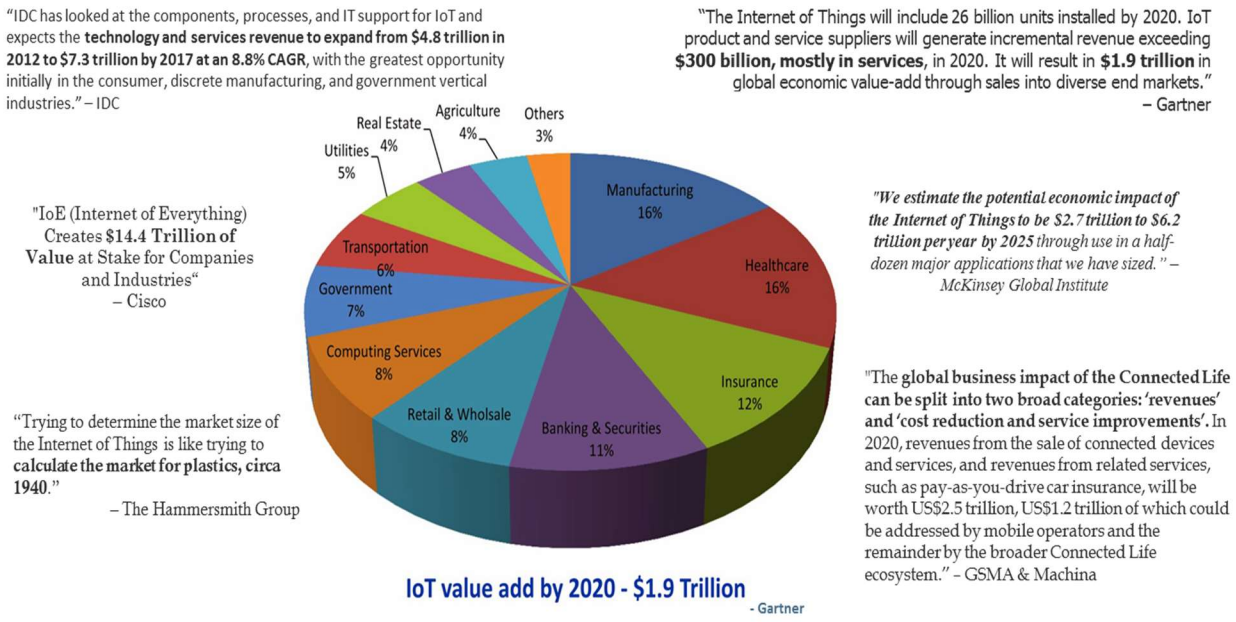
Table of Contents

The Role of the Federal Government in IoT

The Internet of Things (IoT) promises to become a ubiquitous part of citizens' daily lives and organizations' business, changing many aspects of life at home, the workplace, in the community, and across industries. This growth introduces a unique set of challenges, and may indeed represent the most complex evolution of technology we have yet seen. IoT isn't just broadband, telecommunications, cybersecurity, device specification, or data privacy; it brings each of these capabilities and many others together into deeply interconnected systems. As such, solutions for deploying IoT in ways that benefit society and the economy must be multifaceted and engage many stakeholders.

IoT is heavily driven by the rapid advances being made in areas such as sensor development, nano-processing, next generation networking, and data science, to name a few. The pace of technological advancement is rivaled only by consumer expectations—people expect more value out of every interaction they have with devices. Industry analysts have well documented the exponential impact that this explosion of devices will have, as illustrated in Exhibit 1 below.

Exhibit 1. IoT Market Potential



The Federal Government has a unique role to play in facilitating such a challenging landscape. This role can be categorized into the following actions to help shepherd this process:

- Incentivize innovation and R&D for technology companies, academia, and industry consortia
- Provide direct R&D and other scientific understanding of advanced technologies needed to enable IoT that face a market failure and so are not being adequately provided elsewhere
- Promote technological standards to ensure interoperability and promote collaboration
- Support adoption of technologies and standards with pilot programs and other deployments
- Ensure a transparent and enabling regulatory environment for industry to thrive
- Engage in public-private partnerships (P3s) with a variety of commercial organizations

The Department of Commerce (the Department) and specifically its National Telecommunication and Information Administration (NTIA) are uniquely positioned to coordinate the Government's engagement across these arenas. Commerce has a long history of leading policy in technology acceleration, adoption, and standardization. Its Digital Economy Agenda includes a key opportunity of Promoting Innovation, which charges the Department to advance the next generation of exciting new technologies. Encouraging development and adoption of IoT therefore aligns with the Department's historic capabilities and current charge. Further, from complex telecommunications issues to promoting adoption of broadband, NTIA has successfully worked across governments (international, federal, tribal, state, and local) and industry to facilitate coordinated policy perspectives for national progress on technology issues.

Booz Allen Hamilton (Booz Allen) also has a long track record of supporting critical technology issues across the public and private sectors. We have spent decades on the forefront of mobility, communication technologies, sensor development, data analytics, cybersecurity, and the other constituent parts of IoT. Booz Allen's history connecting things and people started decades before the creation of the IoT moniker. Today we have an IoT practice that brings these capabilities together to deploy IoT strategies and solutions, which we've successfully accomplished for Fortune 100 companies and government agencies alike. We create solutions in partnership with industry leaders and start-ups to create, build, and field reusable, scalable solutions anchored in secure platforms with robust and meaningful data analytics.

Booz Allen is pleased to present responses to the set of questions posed by the U.S. Department of Commerce related to IoT and the role of the Department and Federal Government in this field. This response is organized around themes that underscore many of the ways we think about IoT based on our experience developing solutions and strategies with government and corporate organizations. Our response shows the breadth of knowledge on which Commerce may need to rely in planning how it is supported in addressing the expansive needs for coordinating U.S. IoT policy.

Understanding IoT (Q2[1])

The Federal Government's involvement in IoT must begin by considering how IoT is defined. Various and at times conflicting definitions have been proposed by stakeholders. The diversity is often the result of the fact that IoT touches so many different aspects of industry and the lives of citizens and involves a myriad of technologies working together. Differing definitions are therefore the result of differing vantage points within an expansive system. This is reflected in the various terms associated with IoT, which include, among others, the following: cyber-physical systems, physical internet, ubiquitous computing, ambient intelligence, pervasive internet, web of things, wireless sensor networks, physical computing, machine-to-machine, and industrial internet. One can quickly observe that these names, like their corresponding definitions, approach IoT from various perspectives. Some inherently propose IoT as primarily anchored in a particular aspect of an IoT system, including the computing or analytics, physical devices, connectivity, and so forth. The same can be said for the definitions from each vantage point. A "things"-centric view, for instance, will highlight IoT as the deployment of new physical devices and the capabilities they introduce. A computing-centric view, however, would define IoT as the ability to derive

[1] The term "Internet of Things" and related concepts have been defined by multiple organizations, including parts of the U.S. Government such as NIST and the FTC, through policy briefs and reference architectures. What definition(s) should we use in examining the IoT landscape and why? What is at stake in the differences between definitions of IoT? What are the strengths and limitations, if any, associated with these definitions?

new insights from data because there is so much more of it, enabling stakeholders to answer questions we never knew before to even ask. Diversity of vantage points results in diversity of definitions.

Rather than take a particular perspective, the proper definition of IoT must consider the entire ecosystem. IoT can be considered an instantiation of the concept of "emergence" from the field of systems theory, the idea that something like a city, a culture, or even an insect colony can't be dissected *only* into its constituent parts. Rather, a whole greater than the sum of its parts "emerges" in unique ways and must be defined in its own category of evolution altogether. We believe IoT is such an evolution, and therefore any definition must approach it as an ecosystem that sees its function and value resulting from constituent technological building blocks, but particularly as an ecosystem that exists, in a sense, as a thing in and of itself.

As such, we would define IoT as the ecosystem around interconnected sets of devices, sensors, and objects that merge the physical with the digital world. These "things" self-identify and communicate with each other to share and analyze massive amounts of new data to create meaningful insights and action, whether automated machine-led tasks and actuation or human decision-making. The "things" of IoT are everywhere, and include modes of transport such as cars and airplanes, utilities like traffic lights and gas pipes, and even wearable fitness trackers. The value of IoT goes beyond simply connecting these objects to the Internet, but emerges from the ecosystem as its elements work in tandem to recreate how we engage our physical environments. This type of definition adds complexity to working with IoT. For example, through work with commercial energy and healthcare companies, we have seen firsthand that there is no standard reference architecture for IoT that can be used for an organization's decision making or network design needs. Rather, there are variations of a common IoT "stack" that require unique understanding of data flows, security needs, and integration with existing infrastructure to be relevant and useful. We've seen that only an ecosystem view of IoT, rather than it being primarily associated with any one of its technical elements, will lead to a robust and useable reference architecture.

Such an interconnected definition of IoT must be coupled with—perhaps even held in tension with—the fact that the impact of IoT solutions occurs at very specific nodes in the system. We can start by breaking the concept of IoT into consumer IoT (e.g., individuals' use of connected devices for the purposes of wellness, leisure, etc.) and enterprise IoT (e.g., organizations' ability to create new value, safety, and efficiency through wholly new ways of accessing, applying, and leveraging infrastructure and data). Within the enterprise, IoT allows objects to be sensed and controlled remotely across network infrastructure, creating opportunities for cyber-physical solutions that increase safety, security, and operational efficiency while improving resource management and service delivery. These solutions are connecting people to the things around them in new ways, augmenting the workplace for enhanced productivity. In addition, the ability to perform sophisticated computing and processing on devices themselves (i.e., edge computing),

Making IoT Tangible

We've worked with manufacturing organizations that identify tangible value of a particular IoT system in predicting maintenance needs of heavy machinery. Such systems allow manufacturers to maintain equipment during scheduled downtime rather than wait for equipment to break and for the manufacturing line to be shut down before the issue is realized. Zeroing in on tangible outcomes help companies turn an abstract concept like IoT into very tangible sources of value, around which solutions can be designed.

rather than only at a back-end central location, allows for significantly improved response times and information gathering and analyses for planning and operations.

Adopting the emergence definition of IoT—as an ecosystem that is more than the collection of technical elements—while understanding that IoT sees tangible value in specific yet diverse solutions, will allow the Department to appreciate the complex nature of IoT while equipping it to support deployments that realize IoT value through definable systems. Given this complexity, we often recommend to large companies that their new IoT groups should not sit within areas responsible for any single element of the IoT technology stack (e.g., sensors group, network department, or analytics team). Rather, they should establish independent centers of excellence or resource centers that interact with all groups. The Department may benefit from a similarly structured office to facilitate IoT progress across groups.

Overcoming Challenges to Realize Opportunities (Q1, 3, 6, 7, 15, 26, 27[2])

IoT involves technologies and processes that are becoming commonplace in industry, such as sensors, wireless connectivity, and machine learning. However, the combination of these elements into IoT systems leads to an amount of data, a degree of interconnection, and a depth of insights that enable significant economic opportunities. However, technical and policy challenges threaten the value of these opportunities, which the Department and the Federal Government more generally can help to address.

IoT Opportunities

We are seeing particular industries recognize the value of IoT deployment in their market segments. The following include some of the most visible examples that are leaning forward in their IoT adoption:

- **Transportation:** IoT connects and automates vehicles, allowing them to communicate with infrastructure and each other to provide real-time and predictive information about safety,

[2] Question #1: Are the challenges and opportunities arising from IoT similar to those that governments and societies have previously addressed with existing technologies, or are they different, and if so, how? a) What are the novel technological challenges presented by IoT relative to existing technological infrastructure and devices, if any? What makes them novel?; b) What are the novel policy challenges presented by IoT relative to existing technology policy issues, if any? Why are they novel? Can existing policies and policy approaches address these new challenges, and if not, why?; c) What are the most significant new opportunities and/or benefits created by IoT, be they technological, policy, or economic?
Question #3: With respect to current or planned laws, regulations, and/or policies that apply to IoT: a) Are there examples that, in your view, foster IoT development and deployment, while also providing an appropriate level of protection to workers, consumers, patients, and/or other users of IoT technologies?; b) Area there examples that, in your view, unnecessarily inhibit IoT development and deployment?
Question #6: What technological issues may hinder the development of IoT, if any? a) Examples of possible technical issues could include interoperability, insufficient/contradictory/proprietary standards/platforms, spectrum availability and potential congestion/interference, availability of network infrastructure, other; b) What can the government do, if anything, to help mitigate these technical issues? Where may government/private sector partnership be beneficial?
Question #7: NIST and NTIA are actively working to develop and understand many of the technical underpinnings for IoT technologies and their applications. What factors should the Department of Commerce and, more generally, the federal government consider when prioritizing their technical activities with regard to IoT and its applications, and why?
Question #15: What are the main policy issues that affect or are affected by IoT? How should the government address or respond to these issues?
Question #26: What role should the Department of Commerce play within the federal government in helping to address the challenges and opportunities of IoT? How can the Department of Commerce best collaborate with stakeholders on IoT matters?
Question #27: How should government and the private sector collaborate to ensure that infrastructure, policy, technology, and investment are working together to best fuel IoT growth and development? Would an overarching strategy, such as those deployed in other countries, be useful in this space? If the answer is yes, what should that strategy entail?

route efficiency, and environmental considerations. Resulting benefits include vastly reduced wait times imposed by traffic, and almost eliminated fatalities caused by vehicle accidents.

- **Energy**: IoT systems can integrate information from energy providers, the electric grid, and end customers to improve and protect systems by reducing costs and increasing reliability. This includes consumers more efficiently using electricity at home, energy companies better managing energy supply and load to avoid peak prices and outages, and providers addressing grid issues before they occur through real-time data collection and predictive analytics.
- **Healthcare**: IoT enables deeper monitoring and insights of patients and hospital environments. This includes such benefits as remotely monitoring and managing patients after surgery to reduce readmittance rates, tracking doctors to ensure proper sterility procedures to reduce infection rates, and protecting patient data by only allowing access to it from specific locations.
- **Manufacturing:** IoT increases insights into machine performance through plant-wide sensors and dashboards. This can enable predictive maintenance through data science to avoid machinery breakdown, automatic worker tasking through augmented reality, and remote monitoring to avoid sending engineers to remote areas to measure operational parameters.
- **Public Safety**: City-wide IoT can increase awareness for emergency personnel to enhance incident detection and response during crime, disasters, and threats to critical infrastructure. For instance, sensors on light poles can detect gunshots before they are reported and deploy police, and sensors on various floors can identify if there are people in a burning building.
- **Facilities:** Connected systems and predictive analytics can detect room usage, temperature, and other factors that will allow building managers to reduce energy consumption and maximize utilization of resources like meeting rooms.

Whether improving citizen mobility and health, ensuring reliable and sustainable electricity, or optimizing building usage to free up cash for investments, each of the above opportunities help to establish the conditions for economic growth and opportunity in the U.S. economy.

Major Challenges

Opportunities from IoT, including those described above, are evolving quickly as stakeholders seek to derive value from integrating what has previously been viewed as separate systems, devices, networks, and data sources. IoT providers move quickly to secure their piece of the growing market, and their customers seek to benefit from the advantages IoT provides in their deeply competitive industries. Disruption is the norm. Advancements are creating leapfrog opportunities in technology development, techniques for conducting data science, and scores of other capabilities, all while changing the landscape of market players and expectations. We are seeing a wave of not just big industry, but the community of startups and other innovation actors creating ideas and services that improve our lives as consumers, workers, and citizens. However, this pace of evolution introduces significant challenges, thereby creating an opportunity for government to ensure security, interoperability, standardization, incentivization, and innovation for the U.S. market.

The section below explores a number of technology and policy challenges that must be overcome for large scale IoT deployment and its associated economic benefits. Two major challenges, security and privacy, are explored in more detail in later sections.

Technology Challenges:

There are currently no widely accepted IoT **technical standards,** including for edge communication protocols, unstructured data storage, and data management within and among stakeholders. Common

practices are to use proprietary solutions, which are neither standard nor open to allow for flexible use. As such, we have seen many organizations either adopt proprietary platforms and are therefore limited in how they use their own data, or they refuse to lock in their data so are delayed by waiting for open platforms or trying to build their own solutions without an IoT expertise. In some cases, organizations have built their systems with much more complicated optionality (e.g., implementing a dozen different types of proprietary systems) to be ready to adopt whichever one emerges with the agreed upon standard.

Exhibit 2 below lists some organizations and special interest groups that control specific communications protocols and work toward standardization. This is just a sample of the various types of entities that the Department would likely engage as it support the establishment of connectivity standards.

Exhibit 2. A Subsection of Communications Standards Bodies and Stakeholders

Organization	Description
IEEE	Significant work in networking standards.
ISA	The ISA100 committee is part of ISA and was formed in 2005 to establish standards and related information that will define procedures for implementing wireless systems in the automation and control environment with a focus on the field level. The committee is made up of over 400 automation professionals from nearly 250 companies worldwide.
ZigBee Alliance	Open, non-profit association driving ZigBee standards.
RFID consortium	Promotes UHF RFID adoption
NFC forum	Advances adoption of NFC communications
Bluetooth Special Interest Group	Supports collaboration and innovation around Bluetooth technology.
LoRa Alliance	The LoRa™ Alliance Wide Area networks for Internet of Things was initiated by industry leaders with a mission to standardize Low Power Wide Area Networks (LPWAN) being deployed around the world to enable Internet of Things (IoT), machine-to-machine (M2M), and smart city, and industrial applications
Weightless Special Interest Group	Coordinate and enable activities for the Weightless N standard
The Internet Engineering Task Force (IETF).	Community of network designers, operators, vendors, and researchers.
ISO	International Standards Organization
Oasis IoT	Consortium that drives the development, convergence and adoption of open standards for the global information society.
OMA	Open Mobile Alliance was created by consolidating the efforts of the supporters of the Open Mobile Architecture initiative and the WAP Forum. In addition, the SyncML initiative, Location Interoperability Forum (LIF), MMS Interoperability Group (MMS-IOP), Wireless Village, Mobile Gaming Interoperability Forum (MGIF), and Mobile Wireless Internet Forum (MWIF) have consolidated into the Open Mobile Alliance.
OMG	Object Management Group
UPnP forum	Focuses on allowing devices to connect seamlessly and to simplify network implementation in the home and corporate environments.

HyperCat	Aims to create an inclusive one-stop shop of best practice IoT implementation through the sharing of knowledge of processes and applications.

Increased **cyber risks** that are the direct result of increased connectivity and large scale data management and analytics functions, require more comprehensive cyber solutions. Throughout sectors we observe that the relative newness of IoT leaves many businesses without a standard process for building cybersecurity in a uniform way. In a rush to implement a new solution, a business unit will often build an IoT solution then ask the cyber group for sign-off only after it's developed. The pressure to quickly approve new solutions for network deployment, and the lack of industry guidance for how IoT should be treated differently than traditional IT, often leaves cyber leaders asking for a few tack-on cyber measures then approving the deployment. However, controls and protections must be built into solutions from the beginning of the design phase at all levels, from sensors and connectivity to storage and beyond. (See more on cybersecurity below.)

Sensors and edge analytics require new **battery technologies** that don't yet exist. Without improvement, these systems will either be limited in what they can accomplish, or see regular and costly updates and upgrades, both of which may hinder IoT's value proposition. A major oil and gas company recently commented that news articles and vendor conversations give the impression that IoT has fully arrived for oil and gas companies. However, they do not believe that's fully the case. The organization is familiar with sensor deployments, as the industry has been using wired sensors through Supervisory Control and Data Acquisition (SCADA) systems for decades. The newer, cheaper wireless sensors have indeed dropped in price, in some cases from over $20 each to just $1 to $2 in the past twenty years. However, this company hesitated to deploy these wireless sensors because their consistent use in remote locations would result in frequent battery replacements. This is expensive for two reasons: the cost of the battery is high, and it is expensive to send a specialized technician to remote locations. In the case of this company, it was more expensive to deploy IoT for specific remote monitoring solutions because of the battery issue.

There will be heavy and potentially crippling **demand on technical resources like bandwidth and storage.** The challenge isn't novel but its scale is, requiring a rapid deployment of solutions. In the case of bandwidth, next generation networking will help to ease the burden, with advancements like intelligent QoS/QoE, dynamic bandwidth allocation, ultra broadband, and intelligent connected networks. But such advancements won't reach their potential if stakeholders don't learn how to sustainably integrate them. In some cases, for instance, we observe that companies deploy pervasive wireless across manufacturing plants to address IoT's need for more connectivity. However, roll-out across sites is often stalled because those companies haven't yet determined a way to show the return on investment of such connectivity, which is a result of issues around understanding and defining IoT. They simply can't determine what portion of saved costs and increased revenues should be assigned to the connectivity investment versus to historic investments in systems already in place.

IoT is built upon traditional IT and operational systems, which introduces challenges around **integration of legacy systems.** Older systems were not built with an eye toward the technical demands and real-time operations of IoT, either in technology or standards, and so introducing IoT may result in costs and work-arounds that overcome the benefits of the new capabilities. This is often the case with companies that have stores of data from operational historians that log time-based process data for industrial control systems. These systems collected data for decades to be used at specific plants, such as generation plants or refineries. Now that big data offers the potential to uncover system-wide insights

by combining data from across plants, companies are limited by proprietary historian systems. Often vendor solutions don't allow access to data except by other products from the same vendor, which are expensive, or the historian wasn't made to upload the decade's worth of data that sits on it, so doesn't have the capacity to easily transmit. In either case, companies are stuck pulling small stores of their data, unable to take advantage of the big data that their growing IoT systems could otherwise afford.

Policy challenges:
Challenges with implementing IoT throughout the economy extend beyond technology. Those that cannot be solved with more advanced technologies or market maturation will require policymakers to help guide the evolution and remove roadblocks to development. The list below highlights issues that are some of the most important policy-related challenges facing IoT.

- Industry-wide **security** controls and protections should be developed with large scale stakeholder involvement, and ensure no gap in interoperability or backwards compatibility.
- Dramatically **increased privacy data** poses problems as billions more devices collect information. Consumers may have little if any direct interface with system policies except at setup, and so may not realize the extent of data collection. (See more below.)
- At the same time, more stringent reporting and **strict privacy requirements** could hinder some IoT stakeholders from developing IoT technologies. Current laws were based on regulating data in older systems that may not apply to IoT systems with its unique scope and benefits.
- There will be significant **ownership questions around data**. As current trends favor managed services rather than products, consumers may see increasing corporate ownership of consumer data without realizing it (e.g., cloud-based security camera subscriptions versus traditional security camera products with on-premise recording system)

Government's Role in Addressing Challenges

Overcoming these challenges will take time and the involvement of many stakeholders. The Department and the Federal Government in general can take steps now to help move IoT and its benefits forward. The Federal government has already begun to play an instrumental role in working with private industry and research or trade organizations to sponsor, conduct, and support R&D efforts in many areas. Among the most impactful current Federal activities are NIST's thought leadership with the Framework for Cyber-Physical Systems, the USDOT Smart City Challenge Grant, the White House Smart City Initiative, and many cross-agency working groups, initiatives, and research efforts. It is critical that this support and funding continues and that federal agencies take a focused look at what their role in IoT deployments can be, ranging from research and development activities and support to actual implementation of technologies and partnerships with other industry players.

While private organizations are currently addressing many of the technological and governance issues inherent in IoT systems, serving as a central organizing catalyst, promoting access to resources and opportunities for all, and incentivizing interoperability and appropriate security are areas where the Federal Government can play a beneficial role. The Department and Federal Government can provide leadership in IoT and resources to enable others to design and deploy solutions through six primary actions:

1) *Incentivize innovation and R&D for technology companies, academia, and industry consortia.* Due to the societal benefits mentioned above, IoT provides a public good that is under-deployed solely through market activity responding to prices. Through subsidies, tax breaks, grants, and

other financial incentives, the government can make investing in critical IoT technologies cheaper for universities and industry, ensuring that more research is accomplished and IoT' is deployed closer to the societal optimum.

For example, next generation batteries are necessary to power the edge if IoT is going to realize the complex analytics and distributed computing that will deliver its greatest benefits. R&D credits can help to develop the right battery technologies. Such an action would have the peripheral benefit of reducing connectivity needs because more will become possible at the edge, which will help alleviate future spectrum availability issues. Similarly, there is a shortage of data scientists in the market. The government could provide incentives to schools that train these technical experts, or to training programs that produce experts across data science, cybersecurity, engineering, and other technical competencies required in IoT.

2) *Provide direct R&D and other scientific understanding of advanced technologies needed to enable IoT.* The public good of IoT can also be sought through direct research and information of advanced technologies by the government, with the goal of making the resulting knowledge public for industry to rely upon and further. For instance, it can conduct or facilitate research from applicable departments, such as it does with various Advanced Research Program Agencies, or create a rating system around the openness and performance of IoT technologies to reduce the risk and cost of investment decisions for industry stakeholders.

3) *Promote technological standards to ensure interoperability and promote collaboration.* The government can promote open standards and interoperability, primarily through facilitation of standards discussions and by providing supportive information that helps industry consider necessary components. Manufacturers and other key industry players have made progress in this area. For instance, the Open Interconnect Consortium (OIC) and Industrial Internet Consortium (IIC) bring industry, government, and academia together to accelerate an Open IoT Ecosystem with shared architectures, use cases, and taxonomies. These efforts are an excellent start, but much works remains. In the summer of 2014, NIST officially initiated an IoT working group to develop and implement a new cybersecurity framework for IoT - Cyber-Physical System (CPS) Public Working Group (PWG). These efforts seek to address issues such as the identity of the sender; identity of the data; the integrity of the data; and the semantic meaning of the data (including context.) Similarly, the Federal Trade Commission (FTC) held a workshop to discuss IoT-related privacy and security issues. The government should continue to play a central role in facilitating such conversations and supporting industry groups where needed.

4) *Support adoption of technologies and standards with pilot programs and other deployments.* As with personal computers, clean energy, and most other technologies, over time as IoT technology is deployed, it will advance in capability while falling in price. This is because there is more competition to drive down prices, more market incentive to invest in R&D, and more activity to contribute to the body of knowledge that advances the industry. Through pilot projects and general deployment, the Federal government can help industry along this journey. The USDOT Smart Cities Challenge Grant, the USDOT Connected Vehicle Pilots, the White House Smart Cities Initiative, and the DOE's Clean Air Program are all examples of programs that will help deploy IoT solutions, thereby providing learning and best practices that will propel future IoT projects and increase IoT's penetration. Additional technology pilot programs in other industries can follow these examples to further advance research and technology

breakthroughs. Further, the Federal government can influence and accelerate the development of standards through funding such projects. Tying requirements around worthwhile standards to the billions of dollars spent annually on Federal infrastructure and other projects would create significant incentives to ensure interoperability through open protocols, data, architectures and solutions.

5) *Ensure a transparent and enabling regulatory environment for industry to thrive.* Financial markets, including the billions of dollars of investment that are required for IoT to capture opportunities like those discussed above, penalize risk. If investors aren't certain how specific regulations will apply to their investments, or suspect that future regulations could introduce hurdles, they will increase their cost of capital, making IoT projects more expensive. Therefore, uncertain regulatory environments will impede IoT deployments. The Federal government should assess which regulations are overly burdensome or leave too much uncertainty to maximize IoT investments in the market. For instance, we may need to reexamine privacy laws in light of IoT. Companies we serve in healthcare, when exploring IoT to save lives and cut operational costs, are often wary of creating solutions because of perceived risks of using patient data even if rigorously masked. They need guidance prescribing the type and degree of privacy policies that will protect them if they develop and deploy such solutions.

   Similarly, some companies are waiting to adopt IoT until security implications are clearer. The government can help ensure that appropriate security requirements are included in mandated or highly-regulated systems, providing guidance and certification policies for industries to follow to adhere to secure principles. This will drive forward IoT security standards and policies, which can be adopted as best practices across the economy and reduce barriers to entry.

6) *Engage in public-private partnerships (P3s) with a variety of commercial organizations.* Many IoT systems will be extensive in terms of breadth and depth, including large deployments like smart cities. No single stakeholder will have the capabilities to lead these projects alone, and the larger these projects–and therefore the more economy-wide benefits they provide–the more this is true. The funding mechanisms for many such new systems are uncertain, and we believe that Federal government led P3 models make more options available to all stakeholders. For example, in terms of smart cities, Federal agencies could make funding and governance support available to state and local municipalities, where several IoT-type investments will be centered. These recipients can also derive benefits from partnerships with private companies, but they do not often have the extensive partnering frameworks, relationships, and best practices that the Federal government has built with industry.

   The government is also in a unique position to engage the startup community through P3s. Smaller technology companies can provide cutting edge technologies and an agile mindset that will contribute to IoT important solutions in cybersecurity, data services, and analytics, among others. Including these important partners through P3s and other mechanisms will speed the innovation and provide a diversity of thought that can help solve IoT's greatest challenges.

If the Department and other parts of the Federal government can engage in these six ways, the IoT infrastructure and ecosystem across the U.S. will reduce the barriers and allow industry to securely and cost-effectively deploy IoT. As this occurs across industries over time, we will see a broad set of

investments in areas like the opportunities discussed above, with outcomes that strengthen the national economy and help the Department further its mission.

Major IoT Risks: Security and Privacy (Q4, 16, 17[3])

Among the challenges listed above, cybersecurity and privacy issues deserve additional discussion. While most other challenges IoT pose a downside risk of not capturing the full benefit of IoT across the economy, cybersecurity and privacy challenges pose a significant danger of major attacks and data breaches that could altogether overcome the benefit of IoT and leave the economy worse off.

Cybersecurity

Anything connected to the Internet, devices, networks, or back-end systems is a potential vulnerability. Some analysts estimate that 85% of all devices are unconnected and unsecure. As new devices are brought online, new risks surface. Because IoT devices often control physical components, from a car to a pacemaker, security is paramount to ensuring safety and, in some cases, protecting life. Consider how thieves recently used a major department store's networked HVAC unit to hack into payment computer systems and steal 40 million credit card numbers. Perhaps more concerning, cyberattacks have used IoT ecosystems to gain access to critical infrastructure through industrial control systems (ICS). For instance, in December of 2015 an Iranian hacker established remote access to a SCADA system that controlled a hydroelectric dam in New York. The attacker gained access via the system's cellular modem, and gathered information on water levels, temperature, and the status of the assets. SCADA-Access–as-a-Service (SAaaS) marketed through dark web forums, ICS ransomware that locks access to critical systems until a ransom is paid, and other threats are targeting ICS at an increasing rate. Such attacks were higher in 2015 by 15% compared to the second highest year on record, according to U.S.-CERT. Booz Allen forecasts that such attacks will only increase in future years, significantly due to the attack surface expansion through IoT while organizations experience growing pains as they learn how to secure IoT.

Security can't be an afterthought when designing devices or systems – it must be integrated into design in ways we've never required before. Embedded security at the chip level can protect systems from logic and execution attacks. Other security design principles include authentication, authorization, encryption, and ease of updates. Achieving an appropriate level of security not only requires new approaches and products (to include secure gateways), but also educated workforces that can partner with manufacturers to implement secure IoT systems.

For enterprise IT managers, cyber threats have existed in largely two dimensions: behind the firewall and beyond. But with IoT, cyber risk stretches across a third dimension. Employees may come to work

[3] Question #4: Are there any ways to divide or classify the IoT landscape to improve the prevision with which public policy issues are discussed? If so, what are they, and what are the benefits or limitations of using such classifications? Examples of possible classifications of IoT could include: Consumer vs. industrial; public vs. private; device-to-device vs. human interfacing.
Question #16: How should the government address or respond to cybersecurity concerns about IoT? a) What are the cybersecurity concerns raised specifically by IoT? How are they different from other cybersecurity concerns?; b) How do these concerns change based on the categorization of IoT applications (e.g., based on categories for Question 4, or consumer vs. industrial)?; c) What role or action should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to IoT cybersecurity, if any?
Question #17: How should the government address or respond to privacy concerns about IoT? a) What are the privacy concerns raised specifically by IoT? How are they different from other privacy concerns?; b) Do these concerns change based on the categorization of IoT applications (e.g., based on categories for Question 4, for consumer vs. industrial)?; c) What role or action should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to privacy and the IoT?

with a compromised wearable device, or pull their hacked connected vehicle into the parking lot. This creates a new type of cyber risk for organizations, with significantly increased complexity and exposure. As IoT increases the cyber attack surface, organizations must broaden defenses to include the plethora of embedded devices that now make up their ecosystem. We need new security models to protect the entire IoT ecosystem. Smart devices don't have built-in firewalls, anti-virus software, or intrusion detection systems—things that we have on our servers and our desktops. They just don't have the processing capacity to handle that type of overhead. We need standard security models and guidance that can help across the whole lifecycle of IoT from design and build to implementation and operation.

As IoT evolves and new security models and approaches are developed, organizations can apply current security best practices to protect IoT devices and data. At Booz Allen, we take a lifecycle approach to cyber security that includes risk assessment, threat detection, and 24/7 monitoring and risk mitigation. We build in security from the ground-up so that organizations can realize the benefits of IoT while minimizing the risks, using our proven experience developing security solutions for transportation, defense, and other critical industries. Organizations should ensure that IoT devices and systems are implemented to take advantage of existing security protections such as data encryption, firewalls, and access control. Organizations should include IoT devices in their continuous monitoring strategy to maintain ongoing awareness of security threats and vulnerabilities. IoT is happening now and gaining momentum, and it's bringing disruptive innovation to cyber security. Security for IoT must be flexible, agile, and implicit in data sharing. Security isn't merely something built into architecture—rather, it's a living, breathing part of every manufacturing, integration, and user process.

Federal standards and education can help to reduce and address these risks. NIST is taking on a vital role in this area as it proactively works to address cybersecurity with standards, models, and guidance. Initiatives undertaken by major agencies in affected industries such as USDOT, DOE, FHA, and the Department of Commerce have all been instrumental in developing standards, best practices, guidance, and regulations that will guide industries towards more secure implementation of new systems. Continuation of this work and collaboration with industry and other standards setting bodies will be instrumental for the security of concerned and smart systems. The need for research and testing of new cyber solutions will continue to arise as hackers and technical breakthroughs necessitate more and complex security solutions. The government should continue its involvement in cyber security research and implementation as well as around standards, architectures, and guidance or regulations.

Privacy

The deployment of IoT has created a tension between benefits of connecting the 'things' around us and the potential loss of individual privacy. If your phone knows where you work, it can give you directions as soon as you get in the car. If your wearable knows your location and activity level, it can coordinate competitions with your friends and nudge you to be more active. But these solutions may come at the cost of privacy loss. This is a vital conversation with IoT implementation because IoT data goes deeper into the lives of citizens and the operations of businesses than traditional IT systems do. As online adoption grew in the decades after the Internet became widely available, much of our data, behaviors, and information became at risk. The evolution of general connectivity to mobility over the past fifteen years expanded the amount of information online and therefore at risk, and it went a step further by introducing mechanisms to collect wide scale data from our physical worlds, including that of GPS sensors and cameras. IoT increases data collected from the physical world, from citizen driving patterns and biometric information, to business asset maintenance strategies and trade secrets. Privacy concerns of IoT aren't categorically different than past concerns, but they go much deeper.

With the availability of more information and deeper insight about their lives and operations, citizens and businesses will have to possess a deeper understanding of privacy agreements and documentation to avoid opportunities for organizations to collect and/or monetize their data without their knowledge. It is important to help consumers and organizations find the balance between reaping the benefits of connectivity and protecting individual privacy. Individuals and families must have the freedom to choose how much privacy they are willing to concede to enjoy the benefits of IoT. Business and governments should collect the least amount of data possible while enabling users to control settings based on clear understanding of the implications. The federal government may even need to ensure stakeholders understand what they are agreeing to, much like it has done for mortgage lending and other industries.

The federal government should be explicit in how data can and can't be used by aggregators. This will restrict some stakeholders from using data improperly. Perhaps just as importantly, it will also empower other stakeholders—who currently consider some data too risky to use because fines are high and details of restrictions aren't sufficiently clear to act confidently—to use data at all.

Viewing IoT through Citizen Risks

We suggest that the potential downside of cybersecurity should influence how the Department and Federal government more generally categorizes IoT. Because cybersecurity represents a major public policy issue of IoT, and because it is a significant reason why privacy in IoT matters immensely because of its potential to be compromised, we recommend that IoT be categorized through a cybersecurity lens. The Department could classify the IoT landscape based on the public risks faced if data or control is compromised in particular IoT systems. Examples of such categories could include the following:

- Consumer data systems (compromised data risk)
- Public infrastructure systems (downed energy grid, traffic lights, etc.)
- Private industrial systems (localized safety incidents, e.g., plant explosions and downed aircraft)
- Military industrial systems (compromised operations/intelligence)

Such categorization would form the starting point of a useful framework to make decisions that minimize the risks of IoT deployment. Frameworks are necessary when the complexity of an issue benefits from a structured, organized way. This allows stakeholders to break issues into manageable parts to aid in analysis and shared understanding, all while keeping the primary purpose in mind, such as mitigating the risks of IoT.

Impacts on Various Systems and Constituencies (Q8, 14, 19, 22[4])

As the Department decides how it will define IoT and how to promote opportunities while mitigating against risks, it should understand IoT's impact on infrastructure, workforce, and economic equity.

[4] Question #8: How will IoT place demands on existing infrastructure architectures, business models, or stability?
Question #14: What impact (positive or negative) might the growth of IoT have on the U.S. Workforce? What are the potential benefits of IoT for employees and/or employers? What role or actions should the government take in response to workforce challenges raised by IoT, if any?
Question #19: In what ways could IoT affect and be affected by questions of economic equity? a) In what ways could IoT potentially help disadvantaged communities or groups? Rural communities?; b) In what ways might IoT create obstacles for these communities or groups?; c) What effects, if any, will Internet access have on IoT, and what effects, if any, will IoT have on Internet access?; d) What role, if any, should the government play in ensuring that the positive impacts of IoT reach all Americans and keep the negatives from disproportionately impacting disadvantaged communities or groups?

These topics are summarized below, an overview that can help make decisions that protect our primary economic resources while ensuring fair distribution of opportunity and benefit from IoT.

Existing Infrastructure Architectures, Business Models, or Stability

IoT will require changes to existing infrastructure in ways that enable a connected world, including technology shifts, usage of diverse architectures, and efficient use of available resources. For instance, IoT will promote software defined technology and networks, mobile cloud computing, network slicing for custom delivery, dynamic broadband allocation, and integration of heterogeneous networks (e.g., IT and telecommunications technologies). All businesses, even the most traditional, will see the lines blurred between operational technology and information technology, so that all will be forced to become more agile, data driven, secure, and connected if they are going to compete. It will generally be much more plausible for technology firms that already embody these capabilities to pivot to more traditional business lines than it will be for traditional companies to pivot toward a radical technology focus. We are already seeing the makings of this, as newcomer Nest, with its machine learning version of traditional thermostats, is quickly gaining market share in the HVAC sector. Similarly, Google's autonomous car has left traditional auto makers catching up to apply advanced analytics to vehicles.

IoT will also add a layer of precision to public infrastructure that will disrupt procurement cycles and resource usage. For instance, consider two competing implications of IoT in infrastructure. Potholes will be automatically detected rather than reported, and so citizens will expect repair crews to react more quickly. At the same time, street lights that dim when they don't detect motorists may hardly turn on at times but be constantly lit at other times, leaving energy budgets with less clarity compared with the constant usage of the past. Together, these competing trends of added precision pit higher citizen expectations for government with less historical context for the government to make decisions and act. Local governments and other service providers will have to quickly integrate new data streams as IoT deploys, building new baselines to meet increasing citizen expectations.

U.S. Workforce

The way that work gets done is changing, and IoT will continue to be a big contributor to this evolution. IoT offers automated data collection, smart sensors, and intelligent gateways. For instance, inspecting electric meters is completely automatic in many utility service territories. As such, some capabilities or skillsets may become obsolete. As a poignant example of IoT's impact on labor markets, cited by technologist and Wired magazine founder Kevin Kelly, the most common job in the U.S., that of commercial truck driving, may be rendered obsolete as autonomous vehicle technology matures. However, other jobs will grow in demand. In a recent survey of CIOs, 42% of respondents revealed their organizations didn't have the skill sets needed to realize IoT. The workforce will therefore need to adapt. Embedded hardware and software developers, API developers, cyber security officers, project managers and product managers will be key to driving businesses forward. Organizations will need trained data scientists to analyze and remove noise from data, and privacy officers will need to analyze vulnerabilities and evolve policies. Crowdsourcing information will become increasingly popular, as organizations access top talent on demand to conceive new ideas and solutions. This may take flight in augmented and expanded skills, adoption of curated networks, micro-tasking, managing change with complacent staff, and delivering new experiences and incentives to motivate your workforce to evolve. There will also be an increasing demand for the kind of skills machines can't offer, such as emotional intelligence, creativity, and the ability to deduce meaning from information.

Question #22: Are there any Internet governance issues now or in the foreseeable future specific to IoT?

While background computing processes will control more traditional human tasks and organizational activities, IoT will also provide automation that stands to expand our own skills and capabilities. Connected systems within businesses can free up employees' time to focus on high-level, strategic activities. More than that, IoT provides new ways to track information in order to calculate and quantify human behavior more effectively. Happier, healthier, more productive employees who stick around longer—that's the potential benefit of leveraging IoT within the workforce. Organizations that focus too much on bottom-line efficiencies and forced actions may spark backlash, resulting in employee distrust. IoT will require training for employees to learn how to control and manage connected, cross-platform devices. Change management will be critical, but it will also be important to understand new ways to incentivize and motivate employees in genuine ways to meet business objectives.

Industry is not alone in expecting to see dramatic workplace changes through IoT. Booz Allen recently surveyed Federal Government decision-makers across 33 civilian and defense agencies, and results indicated that organizational leaders generally believe they can achieve a number of benefits by transforming their organizations into digital enterprises. A Digital Enterprise is an enterprise that creates and maximizes value to its mission through the delivery of an integrated set of digital technologies, including IoT, to provide additional business value in the form of customer-centricity, increased efficiency, enhanced agility and ongoing innovation.

Therefore, IoT will bring potential job reductions and other costs to the workplace, but it will also introduce incredible benefits through new, skilled jobs and better quality of life. It is imperative that the government promote the benefits, particularly by helping to train experts to take the skilled jobs that will need to be filled. As mentioned above, incentives for education of data scientists, cybersecurity experts, engineers, and other technical experts is a clear role for the government, and can help to protect against the economic growing pains that will surely come with IoT. The Department has already paved the way in workforce training support, particularly through the work of the Economic Development Administration (EDA) and NIST, and recent partnerships with the Department of Labor. Continued investment and incentives for enhanced digital, cyber, and data science training will be critical to ensuring a workforce that is able to build, field, and work within a connected society.

Economic Equity

As discussed above, IoT may negatively affect specific industry segments, and affected workers will often have fewer technical skills and be less educated. This is a real risk, and the government will have to help spur the many new jobs that IoT can help to create. Additionally, though, in terms of equity IoT presents the opportunity to break through existing digital, geographic, and economic barriers in multiple ways, through the advent and implementation of technologies that improve access to key services and opportunities for many disadvantaged communities. Economic progress, underpinned by technology advancement is nothing new to NTIA. The advances in nationwide broadband access and adoption through the Broadband Technology Opportunities Program is just one example of how NTIA has addressed economic disparity through technology advancement. IoT solutions for social good generally fall into three categories: automation, context-aware technology, and remote delivery. All of these areas include immediate support for individuals where they live and work, as well as data science applications to improve social systems in communities and across the nation.

Some examples of current breakthroughs in technology and programs that have improved the lives of and economic/social position of several communities illustrate the benefits that IoT approaches and systems can have on social and economic equity issues.

- Increasing Access for Rural Communities and People with Disabilities with Remote Delivery: In the past few years, there's been significant discussion around telehealth, and the technology available today is nothing short of incredible. Providers can use a combination of high-definition cameras, biometric monitors, and medical devices to not only diagnose but treat some conditions when patients are unable to make in-person visits because of circumstances such as rural locations or disabilities that inhibit movement and travel.
- Connected and Automated Systems Increasing Transportation Access: The movement toward smart and connected cities is enabling the deployment of new transportation and wireless applications that can provide increased access to transportation for the blind, disabled or otherwise marginalized communities. Bridging the digital divide, bringing economic opportunities in the form of access to jobs and information, and providing transport options for those who cannot drive are all excellent examples of ways that IoT approaches are helping to provide not only economic benefits but social equity benefits as well.
- Empowering Older Adults through Automation: The Administration on Aging estimates that by 2040, about 21 percent of the population, or more than 50 million people, will be 65 and older. Of these people, 90 percent indicated in a recent AARP survey that they wish to continue living in their own homes, or 'age in place.' But studies show that older people living alone experience higher levels of disease and disability, as well as higher health and social risks. IoT solutions can help empower older adults to thrive in their own homes, improving their quality of life and decreasing the cost of long-term care.
- Protecting At Risk Infants and Children with Context-Aware Technology: Hospital-grade monitoring systems, such as the Owlet Baby Monitor being developed under a National Institutes of Health grant, could be issued by physicians to not only support families who may be less equipped for parenting, but to enable hospitals to monitor their youngest patients in their homes through secure gateways. In the past five years alone, these types of information and alerts could have helped prevent 110 infant deaths attributed to mothers who used opioids during pregnancy. Expanding similar concepts to toddlers and other young children could help protect the estimated 700,000 victims of child maltreatment each year.

Despite these potential of IoT for underserved communities, the challenges of realizing these benefits for vulnerable and hard-to-reach communities include notably Internet access and financial resources.

- Access to Broadband Internet: Often with IoT, we take for granted that people have access to wireless Internet. However, high-speed wireless can be inaccessible in rural areas and unaffordable for low-income populations. Although the United States is rising in international rankings regarding broadband access, the costs for home Internet and individuals' ability to use the Internet remain barriers for widespread access and adoption. Booz Allen has supported federal efforts to minimize the "digital divide," including the Department of Commerce's $4.2 billion Broadband Technology Opportunities Program. The program funded significant expansion of broadband access to underserved communities nationwide, as well as community training programs to help increase Internet literacy. Another example is the BroadbandUSA initiative to provide assistance to communities wanting to increase their broadband capacity and penetration.

- Financial Resources: Because federal, state, and local governments are often responsible for making the investments to bring new technology ideas to reality, there needs to be an attempt to find the right balance between encouraging disruptive innovations and demonstrating the return on investment necessary to justify public funding. However, communities with less funding, perhaps a small city or depressed region, may not have the public support to launch pilots for smart cities, or subsidies for other projects that would benefit their constituencies. A combination of grants from various federal agencies combined with federally funded pilots, public-private partnerships, and other such interventions led by the Federal government can help to ensure that even these less wealthy areas can enjoy the benefits of IoT.

Impact and Measurement of IoT Systems (Q11 and 12[5])

The government may find it useful to measure economic impact to justify investments in IoT, both from federal agencies and commercial organizations. IoT is complex and interconnected, and the government has a unique vantage point to help address market failures such as underinvestment in coordination. To justify costs of such investments, broad economic forecasts coupled with individual impact assessments of pilot projects could prove very useful.

IoT lends itself to traditional measures and forecasts of economic impact. While the concept can be abstract, a tangible modeling approach can link new data collected and analyzed to the problems being solved and therefore the costs saved, revenues generated, and mission/safety furthered. An economy-wide estimate of economic activity from IoT will therefore look relatively similar to other assessments using traditional methods to forecast the economic benefit of new technologies or industries.

Aside from broad economic forecasts about IoT in general, it is also suitable to assess specific IoT deployments with traditional monitoring and evaluation (M&E) and impact assessments. Experimental design and pilots can help measure the benefits of a solution by isolating outcomes directly resulting from IoT technologies. Traditional methods of impact assessment are adequate, though the interconnection of every aspect of IoT will add complexity to such analyses, with more variables needing to be collected and analyzed. While an impact assessment for a health intervention, for instance, may just need to isolate the impact of a particular medicine compared to a control group, IoT involves the introduction of many aspects and therefore variables, including increased connectivity, new sensors, better analytics, and others. As such, it will be imperative to define what exactly is considered IoT, and how to differentiate it from its constituent parts. This is the primary challenge with IoT impact assessments and must be carefully considered in the design of the system.

The critical element in developing performance measures for any IoT solution is to design a measurement plan when designing and deploying the solution. Measures should be tied directly to intended benefits of the system. While there are many examples in existing industries of how to measure outcomes, IoT may necessitate development of new cross-industry or cross-system measures. This is a good role for the federal government to play: helping commercial organizations consider the impacts of new connected systems, and then developing and implementing processes to measure those impacts. Given the extensive nature and potential benefits of IoT systems, new technical and outcome-based measures will arise. The federal government can use many of its cross-industry working groups or

[5] Question 11: Should the government quantify and measure the IoT sector? If so, how?
Question 12: Should the government measure the economic impact of IoT? If so, how?

stakeholder listening discussions to gather information about what is important and how to use new measures.

International Impacts and Considerations (Q20, 21, and 23[6])

Foreign national governments are actively investing in IoT infrastructures. The UK, India, Dubai, and Singapore are realizing smart city plans to enhance quality and performance of urban services, reduce costs and resource consumption, and improve contact between citizens and government. Smart cities represent a major deployment of global IoT, so it permeates much of the conversation below. Other areas of global IoT include manufacturing, energy, consumer life, and others areas where we see progress in the U.S. Many of these systems are interconnected across the globe. A consumer from the U.S. could, in a single afternoon, drive a connected car in Western Europe that downloads his contact list, use his smart phone to adjust his home thermostat that he forgot to turn down before he left, and use a mirror site based in Asia to watch a video on his smart watch. IoT will be increasingly global as a function of product supply chains, citizen lifestyles, growing wealth, and democratization of content creation. For maximum efficiency, protection, and interoperability, the standards, regulations, privacy protections, and ways in which different governments foster IoT should be coordinated across the globe. NTIA stands well positioned to represent U.S. interests in these forums, much as it already does on other issues via the International Telecommunications Union (ITU). In response to questions regarding how NTIA and the government can best engage internationally, we offer our perspectives on where international coordination will be most impactful and challenges to international regulation.

International Standards Groups: Organizations such as the ITU have stood up IoT working committees (i.e., IoT Global Standards Initiative [IoT GSI], now Study Group 20 of the ITU-T). A key realization of IoT GSI was that there was a need to focus on specific standards to enable smart cities applications. The goal of the new SG20 is to address the need for interoperability of various IoT platforms across industry verticals to better enable the potential of connected, integrated end-to-end architectures applied in smart cities, communities, and other verticals. The ability to play a part of these groups, representing the interests of both the U.S. government and U.S. industries, is an important role for NTIA to ensure that any resulting standards are both flexible to keep pace with future innovation as well as open to ensure market competition and collaboration. There are multiple other standards efforts that have international impact, including efforts led by IEEE, Open Interconnect Consortium, and the Industrial Internet Consortium. NTIA could play a strong role to ensure that the often-viewed as competing standards groups can complement each other so as to balance an open technology ecosystem that can interoperate across vendors and layers of an 'IoT stack' with the needs of data privacy and security.

Challenges to International Coordination: There is much we can learn from the work occurring in other countries, ranging from the smart cities acceleration in the Middle East, protection of privacy in Europe, and emphasis on security being considered in Singapore. It is important, however, to understand the societal context in which these advances are being addressed. For example, when looking to lessons learned in smart cities abroad, we must first consider the governance, financial, and current-state environments. Greenfield advances in areas with no need to leverage existing, complex, antiquated

[6]Question 20: What factors should the Department consider in its international engagement in: a) Standards and specification organizations? b) Bilateral and multilateral engagement? C) Industry alliances? D) Other?
Question #21: IoT Issues for International Engagement: What issues, if any, regarding IoT should the Department focus on through international engagement?
Question #23: Policy Promotion with international partners: Are there policies that the government should seek to promote with international partners that would be helpful in the IoT context?

technologies are an unfair comparison (e.g., comparing digital build out in Middle East cities to the complexities of connecting infrastructures and data in U.S. cities). Likewise, the complexity of our governance models makes the application of lessons learned challenging. To enable a community to take advantage of IoT to improve citizen services in the U.S., we must work with and coordinate decision making across multiple municipal, state, federal, and tribal governments, not to mention organizations from the private sector. Our approach to data privacy is also different than seen internationally, and requires a tailored approach. Notwithstanding the differences in how IoT is applied abroad, the ability to work with and learn from other countries' approaches would still be beneficial. This international collaboration would benefit from NTIA's involvement and leadership.

Other challenges that should be addressed through international coordination include the following:

- Diverse governance models and data localization policies – Governments may require data localization and therefore introduce the inability to conduct broad analyses across countries. Countries may have similarly constrictive data laws, such as dictating what data can be collected and how it can be used, including diverse privacy laws that will add costs as U.S. companies invest in legal teams that can understand the region-specific or even city-specific regulations.
- Lack of technical standards – Just as a stakeholder in the U.S. will find the lack of standards to be a challenge in a single IoT system, companies will find it very difficult to have IoT "systems of systems" across countries because there will be very many proprietary inputs across the world without the advancement of global IoT standards and protocols.
- Lack of data scientists – The application of data science is outpacing the training of professionals in the field. Many countries lack expertise to harness IoT, and U.S. companies seeking to invest in IoT abroad may not find qualified local professionals needed for expansion.

As explored above, through international bodies the government can convene global industry groups to push for international technical standards and communication protocols. This can expand to agreements among governments through multilateral bodies that seek to standardize regulatory policies around data use and availability. The government can also push a data science training agenda through international education and industry bodies, and offer subsidies to universities that provide top programs to train data scientists and give preference to making them available to U.S. companies.

Conclusion

Connecting the physical and virtual enterprise brings exponential potential, from harnessing machine data to increase operational efficiencies, to using remote sensors and augmented reality to prevent injuries and save lives. The volumes of data generated by people, devices, and systems are gateways to smarter infrastructure, increased revenues, and sustainable business growth. But blurring our physical and virtual worlds also brings exponential risk. IoT transcends most organizational structures, requiring thoughtful alignment and collaboration across multiple divisions to develop and implement solutions. Bringing the power of computing to the edge also expands the cyber attack surface, creating new vulnerabilities for systems and networks. And every IoT solution must address new challenges and opportunities regarding systems design and integration, data analytics, and user experience.

Booz Allen combines industry expertise and technical rigor to deliver integrated IoT solutions that solve our clients' toughest problems. We blend digital, cyber, engineering, and analytics together through integrated strategies that consider the organizational needs, industry context, and business opportunities of cyber-physical solutions. Solutions must be integrated throughout the ecosystem of users, software, gateways, and devices. That's why we have brought together experts from across the

firm as we partner with leading computing and software companies to develop end-to-end IoT solutions. Our dedicated team understands business imperatives, combining in-depth industry knowledge with operational expertise to address the toughest IoT challenges. We look forward to bringing these talents and capabilities to bear as you explore the challenges, benefits, and your role with IoT.