IBM

1 New Orchard Road
Armonk, NY 10540-1722

September 9, 2016

Ms. Nakia Grayson
National Institute of Standards and Technology
United States Department of Commerce
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Via Email: cybercommission@nist.gov

RE: Input to the Commission on Enhancing National Cybersecurity
Docket Number: 160725650-6650-01

To Whom It May Concern:

IBM appreciates the opportunity to respond to the topics and questions raised by the Commission on Enhancing National Cybersecurity (the Commission) in the Request for Information (RFI) on the "Current and Future States of Cybersecurity in the Digital Economy". In addition to the topic areas in the RFI, we would like to take this opportunity to describe IBM's expertise in the cybersecurity domain; current and future approach to addressing cybersecurity problems; and provide the Commission a vision to consider when developing recommendations for the next administration and beyond.

Building stronger cyber resiliency with threat sharing

Cybercrime is 21st century organized crime that can affect everyone on the planet. 80% of cyberattacks are driven by highly organized crime rings, with the most sophisticated criminals operating like a well-established global business. These crime rings build development tools, collaborate on software, and share knowledge about targets and vulnerabilities. In fact, each successful attack proliferates the criminals' skills, tools and ecosystems because they often reuse malware and other vulnerabilities that they know are proven to work. While considerable attention is paid to the realm of cyber espionage and nation state activity, the mounting danger of these organized cybercriminals has a significant impact on society.

IBM thinks of cybercrime as a pandemic that can only be stemmed with global collaboration. Consider the rapid and harmonized efforts of the World Health Organization as a virus emerges –information is shared freely and quickly regarding the source of the virus, mode of infection, and rate of contagion. Likewise, cybersecurity must use shared, global data to act as an effective immune system, one that works together to protect the entire entity from contamination, no matter where the “virus” comes from. Sharing information – with speed – is critical. The more threat data that is shared and available in real time, the better companies, governments, and individuals will be protected.

Establishing an immune system also requires the maturity and integration of various security domains: data, applications, network, endpoint mobile, advanced fraud, and identity and access. Security intelligence sits at the center of the system – the central nervous system – aggregating and integrating the data, infusing analytics in each domain to make it stronger.

Depth and Breadth of Security Competency

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security intelligence to help organizations holistically protect their people, infrastructures, data, and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. IBM expertise stems from more than 7,500 hands-on professionals and researchers supporting customers in more than 133 countries. Our deep insight comes from monitoring more than 270 million endpoints and managing 15-20 billion events each day, provided via real-time client feeds and embedded professional engagements. IBM also operates one of the world’s broadest security research, development, and delivery organizations – holding more than 3,000 security patents and leveraging thousands of IBM software engineers, researchers, and consultants residing in 25 security labs around the world, working on security breakthroughs in areas such as cryptography, high-speed data analytics, and identity intelligence.

IBM is at the forefront of threat sharing and intelligent analytics technologies that are used to combat the pandemic of organized cybercrime. Last year, IBM disrupted the traditional business model of threat intelligence by opening to the world its extensive cyber threat research database, IBM X-Force, a 20-year-old vault of 700+ terabytes of security intelligence data. The IBM X-Force Exchange® was created as a catalyst to spark global collaboration against cybercrime[1]. With the launch of the X-Force Exchange, IBM and its global partners have a secure platform to openly share, consume, aggregate, and act on threat indicators from virtually every corner of the globe. This platform assists security analysts in identifying and notifying users about rapidly emerging attacks to help contain and stop the spread of malicious and sophisticated campaigns. To date, IBM X-Force Exchange already has more than 20,000 registered users, including large banks, retailers, healthcare providers,

[1] X-Force is a registered trademark of International Business Machines

automakers, and other industry sector organizations. These users both contribute to and use the database to collaborate with peers and gain insight on attacks. IBM envisions the X-Force Exchange as the foundational platform for threat intelligence and collaboration for its enterprise clients, that include critical infrastructure industries globally, and the industry at large.

Building upon IBM X-Force research and other threat information, IBM recently introduced cognitive computing for security. This technology, called Watson for cyber security, will be designed to sort through, analyze and understand massive amounts of security data – including unstructured data on the Internet – that can overwhelm security professionals today. This includes everything from the estimated 10,000 security research papers published each year, to more than 60,000 security blogs published each month. Our vision is that Watson for cyber security will usher in a new era of cybersecurity by reducing incident response time and time necessary to conduct cyber threat research.[2] This concept is illustrated further in the section on cognitive computing later in this response.[3]

Think Differently About the Cybersecurity Problem

There are barriers that prevent early warning notification systems from thwarting organized crime from operating at their fullest potential. Below are a few tenets for the Commission to consider that may help change the rules of collaboration between government and industry in order to achieve greater success at combating cybercrime.

- In a mutual goal to attain greater cybersecurity, governments around the world need to cultivate public private partnerships and expand the conversations beyond cyber incident reporting policies and focus more on the mechanics of enabling voluntary cyber threat sharing. The Cybersecurity Information Sharing Act (CISA) enacted last year in the U.S. is model legislation that provides legal clarity to ensure the act of voluntarily sharing cyber threat data, in real time amongst and between businesses and government, is protected from liability.

- Public and private organizations need to **democratize** their threat data, meaning that more needs to be shared freely. Democratization of data is possible by eliminating transactional costs to obtaining cyber threat data, or by passing legislation similar to the Cybersecurity Information Sharing Act (CISA), which was designed to help organizations share cyber threat and attack information anonymously and without liability. Sharing rapidly on a massive scale is the only way to counter the sharing at scale of highly organized cybercrime rings around the world.

[2] https://www.youtube.com/watch?v=MYZOIdK4o1M

[3] www.ibm.com/security/cognitive

- Government agencies need to disclose cyber threat indicators, vulnerabilities, breaches and hacking schemes, when appropriate, much faster. Cyber threat sharing is only actionable when it's happening with speed, but most governments are still operating where information remains confidential for as long as possible. With an asymmetric enemy that operates anywhere and with impunity, confidential information is actually working against us. We call this concept the "default declassification of threat data at speed."

Innovation to Stay Ahead of the Problem

The following technology innovation competencies are areas IBM believes will change the fundamental approach to addressing cybersecurity challenges for organizations and governments. As network perimeters disappear with the proliferation of mobile and cloud applications, the analogy of building higher walls and digging wider moats for security is no longer sustainable. While nation state and hacktivist terror activity is certainly of great concern, cyber deterrence efforts need to be focused and centered on the organized crime actors who are behind 80% of attacks, costing the global economy more than $445B a year[4]. It's time to organize ourselves appropriately, think and act proactively instead of traditionally reactively and use the technology tools collectively to beat the bad guys at their own game.

I. Cognitive Computing for Cybersecurity

Cognitive computing is the use of advanced machine learning techniques to understand the meaning of information which was formerly "opaque" to computer systems. This primarily consists of the roughly 80% of the world's information which is unstructured, such as natural human language, images, and video.

Security tools, in broad use today, work primarily on structured or partly-structured, machine-generated information, such as system log and network events. The most advanced security tools apply sophisticated machine learning techniques to identify anomalous events or patterns, and there are tools in wide use that enable searching of natural language (such as text or transcribed speech) for particular content.

A new generation of tools are now being built which augment existing analysis of structured-data with understanding of unstructured-data. This is what is referred to as cognitive security: computing systems which use machine learning to understand the totality of available information relevant to a situation, augmenting the cognition of human beings in order to help them make decisions most effectively.

According to the Ponemon Institute's 2015 Cost of Data Breach Study, 256 days is the average time it takes organizations to detect advanced persistent threats; and $6.5

[4] https://www.csis.org/news/report-cybercrime-and-espionage-costs-445-billion-annually

million is the average cost of a U.S. data breach.[5] Cognitive security will empower security analysts with the capabilities to find early warnings of potential attacks and significantly speed detection. Cybercriminals will find the payoffs to be harder and harder to achieve.[6]

i. IBM Watson for cyber security

The first cognitive security systems focus specifically on cybersecurity: understanding threat information – including unstructured information from the internet – from a wide range of sources in order to bring context to the decision maker. Those decision makers include Security Operations Center (SOC) analysts trying to determine the seriousness of an attack and how to thwart it, as well as intelligence and law enforcement analysts investigating threat actors, campaigns, motivations, and the links between them.

IBM's first such system, Watson for cyber security, integrates with a security incident and event management (SIEM) system to present the SOC analyst views of the data contextually relevant to a security event. For example, if an attack originates with a particular IP address or contains other specific indicators such as a filename, the analyst will see what malware is known to be associated with those indicators; which attack campaigns use that malware; which threat actors are known to employ it; and what has been documented of actors' known associations, intentions, and past incidents. The underlying Watson for cyber security system can be queried to discover these relationships and answer complex questions about the documented evidence of the relationships for law enforcement, intelligence, and counter-terrorist purposes.

Watson for cyber security, and similar cognitive systems, will become key tools for cybersecurity analysis and for security professionals in the future, as threats grow in number, sophistication, and speed, faster than the ability to train security analyst workforces to deal with these attacks. The number of unfilled information security positions around the world is estimated at 208,000 and is expected to grow to 1.5 million by 2020. To continue building Watson's security IQ, and to start training the next generation of security analysts, IBM has begun collaboration with eight universities, including the University of Maryland, Baltimore County. There, UMBC scientists and IBM researchers will push the frontiers of cyber security at the newly created Accelerated Cognitive Cybersecurity Laboratory, slated to open in the fall 2016.[7]

[5] https://securityintelligence.com/cost-of-a-data-breach-2015/

[6] http://cognitivesecuritywhitepaper.mybluemix.net/?cm_mc_uid=99962569066714712716963&cm_mc_sid_50200000=1472820328

[7] http://www-03.ibm.com/press/us/en/pressrelease/49684.wss

II. Blockchain

Blockchain is a technology for a new generation of transactional applications that helps establish security, trust, accountability and transparency, while streamlining business processes. One of the key capabilities of the blockchain is the ability to maintain a record of the history of all transactions in a way that cannot be manipulated.

Not only is it inherently more secure than other types of networks, but blockchain has the potential to be used by multiple parties to share cyber-threat intelligence. Today, for fear of being exposed, some firms are reluctant to share information about cyber-attacks. However, with blockchain, they could confidentially share information in real time that, when combined with data from other companies, could be used to spot patterns and quickly develop countermeasures.

IBM's approach to open source is key to the next phase of enterprise blockchain development. IBM has a long history of commitment to open source innovation and is a premier member of the Linux Foundation's Hyperledger Project, donating tens of thousands of lines of code and helped create the Hyperledger fabric.

IBM was also one of the first organizations to launch highly secure blockchain services and frameworks that may help address customers' regulatory compliance needs across financial services, government and healthcare. Together with our integrated system of analytics, real-time defense and experienced security professionals, IBM works with organizations to select the ideal blockchain solution for their business concerns.

For example, using Blockchain for IoT, an organization can track shipment of a package as it moves along the supply chain by sharing selected logistics and tracking data with relevant partners in the supply chain system. Along the way, required status information can be tracked and shared among all partners in the IoT blockchain.

IBM Watson IoT with Blockchain enables IoT devices to participate in blockchain transactions and automate the execution of business contracts. A private blockchain controls who has access to the blockchain. For example, in the building management use case, data associated with all activities in a smart building from lighting, to climate, to physical access can be tracked.

Blockchain has inherent qualities that provide trust and security, but, to fulfill its promise, the core technology must be further developed using an open source governance model to make it deployable on a grand scale. The federal government must invest in scientific research to accelerate progress. The National Institute of Standards and Technology can help shape standards for interoperability, privacy and security. And government agencies can become early adopters of blockchain applications. In addition, government has a key role to play in certifying the identities of participants in blockchain-based systems.

Commission Topic Area Challenges and Approaches

The Commission requested information on current and future challenges on specific topics. While all the topics are important in their own right and deserve discussion, we felt it was important to share our point of view on critical infrastructure cybersecurity, historically an area of government focus, and the Internet of Things, an emerging area of policy attention and discussion.

I. Critical Infrastructure Cybersecurity

IBM has repeatedly been on public record with the U.S. Government and governments around the world about our belief that securing systems is best accomplished with a risk management approach rather than regulatory mandates and ”check the box” compliance regimes.[8] Some of the reoccurring themes found in our public responses are:

- Regulatory approach does not adequately reflect the ever-changing nature of cyberspace.
- Regulation would also stifle innovation by encouraging firms to invest only in meeting rigid standards or practices that are outmoded before they can even be published and not apply the latest emerging technologies to their cyber risk.
- Businesses must adapt their risk management strategies faster than any regulatory process can move. A static “check the box” compliance regime does not improve an organizations security posture but rather gives an organization a false sense of security.

IBM provides security services and solutions to virtually every sector of U.S. and global businesses and governments. Our expertise indicates that those organizations displaying maturity in security risk management practices have a common characteristic: they have effectively aligned business strategy with security priorities through the leadership of a dedicated, empowered, security executive who manages enterprise security through operation of a pragmatic, risk-based security management program.

IBM values the collaboration and development of the NIST Cybersecurity Framework because it is foremost a risk management program, not a static list of cybersecurity controls. It also provides guidance for all sizes of organizations and the flexibility to adapt to all kinds of cyber risk. Lists of specific controls often do not address the actual risks businesses face every day and cannot keep pace with the world’s constant change. Today’s businesses – which are increasingly dependent on technology for the

[8] http://csrc.nist.gov/cyberframework/rfi_comments/041213_ibm.pdf

http://csrc.nist.gov/cyberframework/framework_comments/20131213_brendan_hannigan_ibm.pdf

http://csrc.nist.gov/cyberframework/rfi_comment_october_2014/20141010_ibm_ignaszewski.pdf delivery of products and services – are particularly subject to the risks associated with swift adoption of rapidly emerging IT-enabled business paradigms. IBM encourages the next administration to continue the public private stakeholder engagement on further socializing the NIST Cybersecurity Framework, to ensure the benefits of its common language and risk management approach to cybersecurity is embraced, not just domestically but globally as well.

IBM recognizes that security for critical infrastructure often goes beyond the business and IT domains. Conventional enterprise IT security measures must be adapted and extended into the industrial process control systems, which involve a myriad of proprietary interfaces, protocols, and heterogeneous devices spread over a large geographic and governance space. One of today's biggest cybersecurity challenges is assuring that IT security controls are applied to these newly connected processes control networks.

Risk management frameworks, organizational structures, and development of secure products are all key components for critical infrastructure security. However, capabilities to receive actionable threat data and appropriately and effectively respond to incidents are just as critical to improve our overall security posture.

II. Internet of Things

Many of the responses below to the questions in this section are reflective of IBM's detailed submission to NTIA's Request for Comment on "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things". We have attached IBM's IoT submission in Appendix A and encourage the Commission to review as well.

1. Current and future trends and challenges

A world of connected things makes the devices, the data they produce and use, and the systems and applications that support them, all potential attack points for malicious actors. And because computing devices take action faster than when humans were "in the loop," there's a potential for quicker spread of misuse and attacks.

Potential attacks include obtaining private or confidential data, manipulating or controlling devices, or confusing or denying service to applications that use and supply data within IoT systems. The risks for IoT systems that support manufacturing, energy, transportation, and other industrial sectors of the economy, are even more challenging. As industrial things become connected to the Internet to enable broader visibility, control, and maintenance, these industrial things also become potential targets of attacks.

A main challenge in IoT is a lack of generally accepted and adopted standards and practices. This includes communications over public and private networks (e.g., mobile carrier standards to support short but frequent packets to and from devices, and standards for local intercommunication between devices) as well as design standards and quality standards for data communications security, etc.

Currently, we see a drive toward time-to-market for connected devices, rather than comprehensive quality and testing (including cybersecurity testing).

2. Progress being made to address the challenges:

- **Standard Framework:** Work is progressing toward a standard framework for developing and managing IoT devices, with security, visibility and failsafe contingencies built in.
- **Cognitive Computing**: Cognitive security uses machine learning to understand the totality of available and relevant threat information, which will help combat the evolving nature of threats in IoT.
- **Predictive analytics:** Because of their ability to transform massive amounts of data into actionable intelligence, predictive indicators can identify new emergent risks even before they result in significant losses and can help security analysts prioritize alerts.
- **Behavior-based security analysis**: Analysis that identifies typical and atypical behavior can help prevent misuse, and policy-based automated responses can be put in place to act on these observed behaviors. Once there's a successful response in one geo-physical area, it can be applied to other areas in order to prevent similar attacks before they are observed.
- **Standards for design and testing**: Standards are helping to ensure that security is built into design. Testing for exploitability via threat modeling, testing prototypes, and penetration testing for final delivery units should be required

3. What can or should be done now or within the next 1-2 years to better address the challenges?

Organizations responsible for IoT systems must understand how all this data will move – from device to device, across data centers, and even across borders – and develop security and privacy protocols that will reliably collect, protect, and dispose of data in a manner that appropriately manages risk and achieves compliance with regulatory obligations. Manufacturers must develop methodologies to update and patch any system that connects to the Internet over the wire and for its anticipated lifetime.

Existing standards groups, such as ISO, NIST, ETSI and CERT provide excellent support in recommending approaches for secure processing and handling of data as well as handling vulnerabilities, security incident responses, and incident disclosures.

Existing and in-progress guidelines, recommendations, and standards, coupled with business and industry groups such as Information Sharing and Analysis Centers (ISACs), should be used to continue to innovate and extend security into IoT systems.

Understanding that IoT results in vastly larger amounts of human-related information collected by intent (e.g. fitness, healthcare) or inadvertently (sensors ranging from microphones and cameras to thermometers and GPS receivers), industries must establish reasonable and appropriate policies for handling this personal information.

As we develop these approaches for secure and private processing of IoT data, we must build in security and privacy by design, and promote trust and transparency, in developing and implementing IoT. Technologies, such as Blockchain for IoT, can ensure that contracts for privacy and data sharing are met and can be confirmed as needed by all parties.

4. What should be done over the next decade to better address the challenges?

Governments and private industry need to create a world-wide early warning system – based on real-time sharing of intelligence - for attacks, vulnerabilities, and protections of cyber-security threats.

As we have discussed in this submission, cybercrime has grown rapidly, due to its organization and collaboration, to become one of the most challenging issues of the digital age. While intelligent cyber security systems are fast advancing, as demonstrated in cognitive computing and blockchain technology, private and public organizations need a new mindset that includes democratizing and collaboratively sharing threat data to help fight back at scale.

Governments need to help support threat sharing by declassifying data at speed, when appropriate, to help organizations collectively understand and defend against attacks at much greater speed.

IBM applauds the Commission and NIST for their work and commitment to the stakeholder engagement to improving our cybersecurity posture. Please contact Katie Ignaszewski in IBM's Government and Regulatory Affairs office for more information or questions at 202-551-9372 or kignasze@us.ibm.com. We look forward to the Commission's recommendations and working with the next administration and government partners.

APPENDIX A

1 New Orchard Road
Armonk, NY 10540-1722

June 2, 2016

Mr. Travis Hall
National Telecommunications and Information Administration
United States Department of Commerce
1401 Constitution Ave., N.W.
Room 4725, ATTN: IOT RFC 2016
Washington, DC 20230

Via Email: iotrfc2016@ntia.doc.gov

RE: The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things
Docket Number: 160331306-6306-01

Dear Mr. Hall,

IBM appreciates the opportunity to respond to the Department of Commerce's Request for Comment on the "Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things."

A. Introduction

The billions of connected things around us are helping drive a new digital revolution that is transforming every part of society, every sector in industry and the entire government apparatus. The connectivity of things that enrich our lives, businesses, and organizations, such as investment in a smart thermostat, medical devices, automobiles, and industrial equipment, presents an exciting environment for innovation, new business opportunities and societal benefits.

IBM recognizes that the Internet of Things (IoT) is radically changing the way businesses operate and people interact with the physical world. Through our Watson brands, we are helping bring the power of cognitive computing to address the challenges of extracting and analyzing data embedded in intelligent devices in real time. IBM has been developing a new generation of cognitive systems that have visibility to analyze the massive amounts of data that have previously been hidden and untapped.

Cognitive systems have the capability to inject a form of reasoning ability into every digitalized object, process and service. IBM is leading the IoT movement globally - with 750 IoT patents, 300 researchers dedicated to IoT and, 9 global client experience centers. IBM is a trusted provider with leading IoT and security expertise and we are actively engaged with our clients to seize the opportunities that IoT presents across industries around the world. Thus, we have the practical experience with IoT to provide what we hope will be a helpful point of view on the government's role in fostering its advancement.

IBM's responses to the Department of Commerce's specific questions are in Section B (Responses) below. We answered only the questions to which we felt we could lend value and expertise. Before addressing those specific questions, however, we would like to set forth a few themes, which we believe should guide the Department of Commerce's general analysis of IoT:

1. Governments should adopt a "wait-and-see" approach before introducing any IoT-specific regulation.

The pace of IoT-related development is extraordinary as exemplified by the innovations in cognitive computing. Many of the issues that IoT raises, such as privacy of peoples' information, are already addressed by existing laws and regulations, and stakeholders are already working to understand how these existing frameworks should apply to IoT. Because the technology and use cases in this space are rapidly evolving, prematurely imposing regulations could stifle innovation. IBM proposes the Department of Commerce consider that any existing gaps in regulations could be worked through in the marketplace via contracting, self-regulatory frameworks, open standards and competition.

International cooperation amongst governments to identify common areas of interest, discourage broad data localization policies and enable standardization priorities would benefit emerging technologies, including IoT. It would also avoid fragmentation and future disagreements that would hamper opportunities for companies to scale IoT solutions world-wide.

2. Policymakers should encourage security and privacy by design, not only to promote flexibility in creating IoT solutions but also to optimize security and privacy protections. Government should not mandate the details of such implementations.

The threats faced by organizations change daily, and the threats confronted by one industry sector can be significantly different than those faced by another. Given the constantly evolving nature of cyber-threats, responding to them requires great speed and agility, practical risk-based management, and innovative defensive measures. A set of security and privacy principles is better able to keep up with the challenges to and changes of technology in the marketplace than any given set requirement. It is not about just flexibility in creating the IoT solution itself, but the ability to quickly adapt on security and privacy. The NIST Cybersecurity Framework, developed in tandem by the government and private sector, illustrates that rather than dictate specific technologies, measures or outcomes, the Framework establishes a common language for organizations to evaluate their cybersecurity posture and to identify and prioritize opportunities to improve it. Because the Framework is designed to be adaptable to organizations of different types and sizes, it can be customized to an individual organization depending on its risk profile, resources, and needs. IBM believes the NIST Cybersecurity Framework public private partnership is an example of a reasonable and foundational model going forward for policymakers to utilize for discussions around securing IoT architectures and systems and privacy.

Standards organizations (e.g.: ISO, NIST, Industrial Internet Consortium (IIC), Open Interconnect Consortium (OIC), ETSI, AIOTI), including several of which IBM is a member, have already been discussing best practices for security and privacy by design for IoT. Many of these practices are not new to IoT, but are recognized development and deployment practices that have been created and refined even before the rise of IoT.

3. Governments should protect the free flow of data to support the growth of IoT. Data is the lifeblood of the global economy. In today's connected world, international commerce simply cannot function without constant streams of data flowing across borders. The free movement of data allows U.S. companies of all sizes and in all industries to bring new innovations to global markets, driving investment, growth and job creation. Cross border data flows particularly enable small and medium-sized enterprises (SMEs), to compete in the global economy. Access to digital products and services, such as cloud applications, provides smaller companies with cutting edge services at competitive prices, enabling them to participate in global supply chains and directly access customers in foreign markets.

Unfortunately, governments around the world are considering or are already imposing digital trade barriers. Both U.S. companies and those in countries with localization requirements have a lot to lose if these barriers are not addressed. To support the growth of IoT and the continued competitiveness of the U.S. economy, the U.S. Government should aggressively protect cross border data flows through bilateral and plurilateral trade agreements. The Trans Pacific Partnership (TPP) includes new and innovative disciplines protecting the legitimate flow of data across borders. The Trans-Atlantic Trade and Investment Partnership (TTIP) and the Trade in Services Agreement (TiSA) provide important opportunities to build upon these TPP disciplines and help right the "rules of the road" for future trade agreements. Specifically, these agreements must include binding provisions protecting cross border data flows and preventing "data localization" through requirements to use local data centers. In any event, privacy and security considerations in IoT systems can be addressed without data localization.

4. “Open” is key for IoT adoption. The task of connecting billions of devices among a multitude of stakeholders is complex, to say the least. Open standards in terms of connectivity of devices and networks is critical, and it will enable interoperability. Open

source tools and capabilities enable a wide range of people and companies to enter the market and IoT ecosystem.

5. Promote innovation and competition. This is an exciting and transformative time given the advent of IoT. Many of the possibilities and challenges that come with this technology are still unknown. Accordingly, when new issues arise as IoT matures, it is important that the governmental response to such issues remains open to flexibility and encourages continued innovation and competition.

B. Responses

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?*

Similar Challenges

- System interoperability: System interoperability - the ability of "things" to communicate with each other clearly and efficiently - is always a challenge that must be addressed in technology. Because the IoT is a more complex and widely spread system, interoperability is fundamentally important for the IoT ecosystem to grow.
- Security: Security has always been critical to any technology. The rise of IoT heightens that importance due to the closer coupling of digital and physical environments that IoT provides.
- Privacy: Just as existing law and principle have been brought to bear on previous technological advances, existing approaches will remain relevant to IoT. For example, safeguarding privacy will require privacy and security by design throughout the product and systems development lifecycle. At the same time, principles must evolve with technology; notice-and-choice is a frequently discussed example. Because new IoT implementations will raise new issues, a principles-based approach through specific design processes will produce better results for both privacy and innovation than new, IoT specific requirements that will likely have unforeseen and unintended consequences.
- Liability: Liability risks relevant to IoT are not new or specific to IoT. While IoT technologies create interdependencies between multiple product developers, service providers, data users and end users, these interdependencies already are present for other existing types of technology that are included in complex supply chains. Thus, there are existing legal frameworks to address liability in these contexts. We do not see a need for new "IoT" liability rules. An additional complexity could be created with fully autonomous systems, such as self-driving cars, but also here it is important to carefully assess the situation and identify problems before moving forward with developing new rules or modernizing existing rules.

Different Challenges

- Security: IoT definitely expands the scope of security issues that companies and end users now have to confront. A world of connected things makes the devices, the data they produce and use, and the systems and applications that support them, potential attack points for malicious actors. Potential attacks include obtaining private or confidential data, manipulating or controlling devices, or confusing or denying service to applications that use and supply data within IoT systems. The risks for IoT systems that support manufacturing, energy, transportation, and other industrial sectors of the economy, are even more challenging. As industrial things become connected to the Internet to enable broader visibility, control, and condition based maintenance, these industrial things also become potential targets of attacks. To summarize, the points on different security challenges are:

- More devices (systems/endpoints/nodes)
- Those devices have a wide range of characteristics (e.g. low to high processing capacity, small to large memory and power consumption limitations)
- More data, and new kinds of data
- Devices are directly connected to and can directly change a physical environment

To help protect these systems, the system and those responsible for it must understand how that data will move – from device to device, across data centers, and even across borders – and develop security and privacy protocols that will reliably collect and protect data in a manner that appropriately manages risk and achieves compliance with regulatory obligations. Existing standards groups, such as ISO, NIST, ETSI and CERT provide excellent support in recommending approaches for secure processing and handling of data as well as handling vulnerabilities, security incident responses and incident disclosures. Existing and in-progress guidelines, recommendations, and standards, coupled with business and industry groups such as Information Sharing and Analysis Centers (ISACs), should be used to continue to innovate and extend security into IoT systems.

Different opportunities

IoT technologies offer numerous new and different opportunities than existing technologies. We provide a few examples here.

- Cognitive IoT: Cognitive systems are those that understand, reason, learn, and propose action and that are intended to augment and expand the scale of human expertise. In contrast to some characterizations of artificial intelligence, these systems do not replace human expertise. The traditional approach to programmable computing – in which data is shepherded through a series of pre-determined, if/then processes to arrive at outcomes – cannot process the degree and kind of data needed to fulfill the promise of IoT. Programmable systems thrive on prescribed scenarios using predictable data. This rigidity limits their usefulness in addressing many aspects of a complex, fast-paced world where the value of data decreases exponentially every second it goes unused. Rather than being explicitly programmed, cognitive systems learn from interactions with humans and their experiences with their environment. This enables them to keep pace with the volume, complexity, and unpredictability of information generated by the IoT. In addition, cognitive systems can make sense of the 80 percent of the world's data that computer scientists call "unstructured" – like videos, audio, even blogs and social media.[9] Unstructured data is data in a format that requires some type of interpretation in order to reveal the information found within it. One of the powerful elements of cognitive computing and cognitive IoT is applying machine-based interpretation of IoT sampled data (i.e. unstructured data) and revealing information from that data. That means we are now able to illuminate aspects of the IoT that were previously invisible – patterns and insight culled from disparate sources – allowing people to make more informed decisions.

- Blockchain: Use of blockchain technology can also be applied to IoT applications. Blockchain is a technology for a new generation of transactional applications that establishes security, trust, accountability and transparency while streamlining business processes. A blockchain has three main components.

  1) A network or group of parties, where members of that network or group transact business.

  2) A shared ledger in which every transaction in the network is permanently recorded. Each member possesses a copy of the encrypted ledger and once a transaction is recorded it is virtually impossible to manipulate because each transaction must be validated by all or a majority of the members. In fact, cryptography and digital signatures are used to prove identity and gate access to the shared ledger.

  3) A set of defined transactions which run in the blockchain network. This is the digital representation of the terms of an agreement.

IoT applications can be integrated into the blockchain transactions to automatically fulfill the terms of the agreement, which members have agreed to, without human intervention.

For example, equipment manufacturers, parts suppliers, and maintenance companies might create a blockchain-based system for holistically managing all of the collective handling of parts and components used and serviced. With real time IoT data from connected IoT devices, the group can automate the execution of transactions based on the agreement among its suppliers. All of the suppliers will share the exact same information about a new equipment model – every step in the process of planning, designing, assembling, delivering and maintaining it. One of the key capabilities of the blockchain is the ability to maintain a record of the history of all transactions in a way that cannot be manipulated. This history can not only help resolve any disputes that may arise but can also help to demonstrate compliance with government regulations as well as internal rules and processes.

[9] Holzinger, Andreas; Stocker, Christof; Ofner, Bernhard; Prohaska, Gottfried; Brabenetz, Alberto; Hofmann-Wellenhof, Rainer (2013). *"Combining HCI, Natural Language Processing, and Knowledge Discovery – Potential of IBM Content Analytics as an Assistive Technology in the Biomedical Field". In Holzinger, Andreas; Pasi, Gabriella. Human-Computer Interaction and Knowledge Discovery in Complex, Unstructured, Big Data. Lecture Notes in Computer Science. Springer. pp. 13–24. doi:10.1007/978-3-642-39146-0_2. ISBN 978-3-642-39146-0.*

a). What are the novel technological challenges presented by IoT relative to existing technological infrastructure and devices, if any? What makes them novel?

Autonomous Products: Fully autonomous "things", like self-driving cars and robots, present novel safety challenges related to security, connectivity and availability. If human oversight and management of a device is not possible, then the device should be designed to be "hardened" and protected in order to mitigate against the risk of hackers, interoperability problems, and down-time. This is necessary in order to protect the physical safety of people and the environment in the vicinity of the device. IoT devices and systems should be designed to gracefully degrade their level of service as well as recover, and be prepared for changes, all without requiring human assistance. Even when devices are disconnected from a network, they need to be designed to be secure and to operate for their intended purpose. Further, IoT devices must be able to detect attacks and take appropriate actions to defend against such attacks.

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?

A primary challenge to policy is to assess and clarify the application of existing regulations to IoT, and only develop minimum regulations necessary to fill any gaps needed to promote privacy, safety and security while fostering innovation and competition. The global nature of the digital environment highlights a need for interoperability and consensus on regulations and standards which allow for world-wide usage and deployment.

c). What are the most significant new opportunities and/or benefits created by IoT, be they technological, policy, or economic?

IoT is fundamentally changing the way businesses create value, companies compete and partner, and consumers experience the world. On their digital transformation journeys, companies are digitizing transactions, interactions, and much of our physical world, opening new opportunities for insight, relevance, and innovation. The Internet of Things has made the leap from conceptual to actual.

- Size and Scope: Nearly 13 billion connected devices will grow to over 29 billion by 2020.[10] These devices improve our everyday lives with personalized, responsive experiences and generate valuable data and insight that will help solve problems at a global scale.
- Measurable value: Data from IoT will yield insights that drive economic value of

[10] IDC,"Worldwide and Regional Internet of Things 2014-2020 Forecast Update by Technology Split," Doc #252330, Publish date: Nov 2014. http://www.idc.com/getdoc.jsp?containerId=252330

more than $11 trillion by 2025.[11] B2B users will generate 70% of this value, mostly through operational efficiency gains from initiatives like smart factories and connected supply chains. IoT enables better decisions and, where appropriate, automated actions.

- Rapid Adoption: 82% of enterprise decision makers say IoT is either strategic or transformative to their industry.[12] Industry disruption is beginning and will accelerate as connected objects become active participants in our economy. IoT adoption will spur new business models, turning more companies into technology and services companies.

By bringing together the physical and digital worlds, the IoT vastly expands the reach and impact of information technology. With this phenomenon comes an enormous surge of data. IoT data is growing twice as fast as social and computer-generated data—and yet most IoT data is never acted upon – thereby presenting a data challenge.[13] It may be too big and expensive to store and move, may need to stay out of the cloud for legal or other reasons, may be too complex to analyze and act on in real-time, and too challenging to combine with other data sets such as weather. Cognitive overcomes the limits of programmable computing and will be able to keep pace with the IoT complexity and data growth. More devices means more sensor data to process from multiple feeds and to look simultaneously at multiple streams of data – activity that is just not feasible for humans. This requires computation in order to sort out and summarize information so that it can be readily acted upon. Some examples are:

A car that adapts itself to individual driving style and current road conditions;
A building that manages its temperature, lighting, and power consumption to save energy;
Factory equipment that predicts its own service needs and requests maintenance to avoid downtime;
A retail store that provides shoppers with customized offers and enhanced shopping experience;
A transportation system that anticipates demand, avoids congestion, keeps travelers informed, and improves safety.

2. *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.[14] What definition(s) should we use in*

[11] Unlocking the potential of the Internet of Things. McKinsey & Company. June 2015

[12] IDC,"Worldwide and Regional Internet of Things 2014-2020 Forecast Update by Technology Split," Doc #252330, Publish date: Nov 2014. http://www.idc.com/getdoc.jsp?containerId=252330

[13] Unlocking the potential of the Internet of Things. McKinsey & Company. June 2015

[14] Federal Trade Commission, *Internet of Things: Privacy and Security in a Connected World*, FTC (Jan 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-of-things-privacy/150127iotrpt.pdf; Abdella Battou, *CPS PWG: Reference Architecture*,

examining the IoT landscape and why?

The use of connected devices crosses and touches numerous industries and disciplines, including both consumer facing and industrial facing applications, resulting in many ways to characterize IoT. This is also illustrated with NIST and FTC definitions. At IBM, we refer to the Internet of Things, or 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. For consumers, these devices include mobile phones, sports wearables, home heating and air conditioning systems, vehicles, and more. In an industrial setting, these devices and sensors can be found in manufacturing equipment, the supply chain, and in-vehicle components.[15]

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?

Trade Policy: For the first time under the 2015 Trade Priorities and Accountability Act, the United States Trade Representative is required to negotiate protections for U.S. companies against data localization requirements in trade agreements. As noted earlier in this submission, cross border data flows are critical to the ability of U.S. companies in all sectors to operate and compete in the global economy. Requirements to localize data and computing facilities undermine data-driven innovation and increase barriers for global companies that rely on data to operate and compete. Ensuring that future trade agreements include protections against these requirements is vital to U.S. competiveness, particularly in the field of IoT.

Existing legal frameworks: As stated previously, many of the issues related to privacy and liability are already addressed by existing frameworks and is premature for governments to adopt IoT-specific regulations.

- Privacy: Existing federal and state regulations, as well as those bearing on certain types of data, already robustly regulate the handling and protection related to end users' private information and provide recourse for data breaches. Further regulation in this area is not needed and, if IoT-specific regulation is imposed while IoT technology is at the nascent stage, such actions could stifle innovation. At the same time, improvement to existing laws and regulations could benefit IoT as well (e.g. a federal data breach law with preemption).

- Liability: Liability risks discussed with respect to IoT are not new or specific to IoT. Even though IoT creates interdependencies between multiple "things" or products,

National Institute of Standards and Technology (accessed March 9, 2016), http://www.nist.gov.cps/cpspwg_refarch.cfm

[15] http://www.ibm.com/internet-of-things/learn/library/what-is-iot/

> service providers and end users, that is also true for other types of technology and services with complex supply and value chains, such as outsourcing and vertical manufacturing processes, e.g., assembling an airplane. Thus, the well-established existing legal framework is fit to address liability issues in the field of IoT and we see no need for new liability rules for data. Existing tort law imposes liability for damages caused by products with design defects or manufacturing defects.

Security Testing and Coordinated Disclosure of Vulnerabilities: Enabling responsible and lawful security testing as well as the responsible and coordinated disclosure of found vulnerabilities to IoT manufacturers is an important way to foster IoT. Supporting a public discussion around these topics with an eye toward resolving conflicts is a role that might be played by governments.

As for security testing of IoT, in late 2015 the Library of Congress' rulemaking efforts resulted in a broad debate as to whether such security testing is appropriate, and resulted in the creation of a three-year exemption to The Digital Millennium Copyright Act's (DMCA) anti-circumvention provisions that allows for some "good faith security research" of computer programs included in consumer devices.[16] Such testing is limited to computer programs within lawfully acquired devices or machines, and is subject to current law, including the Computer Fraud and Abuse Act, which among other things prohibits unauthorized hacking of systems. It defined "good-faith security research" as meaning *"accessing a computer program solely for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability, where such activity is carried out in a controlled environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement."*[17]

We believe rules, such as testing in a controlled environment to avoid harm and a purpose to promote security and safety, are an important beginning to establishing lawful and careful approaches to security testing of IoT devices. However, given the limits of DMCA itself, this is not a complete approach to this subject and we believe further public discussion is needed to establish appropriate permissions and limitations on lawful security testing.

We expect there will be value in competition for monitoring, certification, and testing, much like the existing testing and certification for electrical and electromagnetic specifications. Government should encourage the use of existing industry standards, testing, and certification of services provided by a competitive private industry.

[16] http://copyright.gov/1201/2015/fedreg-publicinspectionFR.pdf

[17] http://copyright.gov/1201/2015/fedreg-publicinspectionFR.pdf, page 51

The DMCA's exemption does not provide for how security vulnerabilities, if found, should be communicated to the manufacturer or others. This is referred to as "coordinated disclosure" or "responsible disclosure," i.e., the practice of sharing found vulnerabilities between researcher and manufacturers in such a way as to minimize dangerous impact to consumers or the community. How to conduct a proper "coordinated disclosure" is a topic of debate today. As traditional industries transform their business models around IoT, they will also have to understand and collaborate with the vendor and research communities in order to keep their systems and devices secure. Existing avenues utilizing self-regulating industry groups may need to expand in order to encourage prompt and effective coordinated disclosure.

A positive development in this area is the creation of IoT CERT for cyber-physical problems. This CERT is convening stakeholders from various industries to establish recommendations and guidelines to build trust among community members and to improve security overall. Certainty and trust as it pertains to security vulnerability handling as well as a coherent approach will help with adoption of IoT and provide a level of understanding of the protection that vendors are providing in the face of constant threat activity.

b). Are there examples that, in your view, unnecessarily inhibit IoT development and deployment?

I. Recently, the Department of Transportation National Highway Traffic Safety Administration (NHTSA) issued an Enforcement Guidance Bulletin on Safety Related Defects and Emerging Automotive Technologies that could affect hardware, software or devices installed in, or connected to a vehicle.[18] It is an example of the convergence of cyber and physical security issues with overreaching policy recommendations that could be more harmful than helpful. Through the guidance, NHTSA was considering software to be motor vehicle equipment and thereby subject to reporting all safety related defects to NHTSA under the National Traffic and Motor Vehicle Safety Act. This broad interpretation could result in all software vulnerabilities being considered "defects" for reporting purposes, whether or not they caused a safety issue within a car. The broad scope of NHTSA's guidance could set an inaccurate and confusing precedent for other industries looking to adopt IoT.

II. As indicated in the introduction, governments around the world are considering or are already imposing digital trade barriers. U.S. companies have the most to lose if these barriers are not addressed. Cross border data flows must be preserved through bilateral and plurilateral trade agreements as seen in the E-Commerce Chapter of the Trans Pacific Partnership (TPP) that outlines essential disciplines for continued realization of the potential the digital age offers, IoT being one area. IBM is hopeful that

[18] https://www.federalregister.gov/articles/2016/04/01/2016-07353/request-for-public-comments-on-nhtsa-enforcement-guidance-bulletin-2016-02-safety-related-defects

Congress will pass TPP this year and pave the way for continued innovation and U.S. leadership in the global market.

5. *Please provide information on any current (or concluded) initiatives or research of significance that have examined or made important strides in understanding the IoT policy landscape. Why do you find this work to be significant?*

IBM has a long history of innovation and research in IoT. We are currently deeply involved in IoT Security for Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) systems, including cognitive security innovations to provide a robust solution to the complexity of this space. We are researching the use of blockchain, as a means of addressing open, secure and scalable solutions for both general and industry specific innovations across the IoT. We are also considering integration of disparate data sources for cognitive solutions to address grand challenges like: global food production, clean energy production, and healthcare. The IoT allows for IBM, our partners and our customers, the opportunity to transform businesses and have positive impact on the lives of millions around the world.

8. *How will IoT place demands on existing infrastructure architectures, business models, or stability?*

IoT will result in more data, processing, communications, storage, and a potential decrease in traceability between cause and effect. This could happen in two ways: (1) logic "dispersion," where the logic for carrying out an action is spread across elements running in a variety of locations, environments, and programming language; (2) logic completely "dissolved," into machine-learned decisions. Even today, it is often hard to determine the precise location of a problem in a system since individual elements may all act and operate as expected but still result in undesirable or incorrect behavior. The complexity of IoT interconnected systems and devices can exacerbate this challenge.

9. *Are there ways to prepare for or minimize IoT disruptions in these infrastructures? How are these infrastructures planning and evolving to meet the demands of IoT?*

If all devices start communicating at heavy rates and deployment out-paces networking, then systems – including safety critical systems – could be adversely impacted. For example, we expect that safety services such as fire, law enforcement, and emergency services will increasingly depend upon information provided by IoT systems. Accordingly, IoT offerings for those services should be designed and implemented with high availability and security redundancies to mitigate risk of failure.

IoT platforms are the control points for overall IoT operations. They collect, integrate, and otherwise manage the data itself and structure the processes that will be used to analyze that data. These platforms should be built to handle multiple data streams from disparate sources and need to implement privacy by design and security by design. Elastic cloud infrastructure should be built to absorb the increased burden of data and computation requirements. Cloud providers must actively manage the growth of data, communications, and processing on their systems.

15. *What are the main policy issues that affect or are affected by IoT? How should the government address or respond to these issues?*

A few years ago, Ginni Rometty, Chairman, CEO and President of IBM, declared at the Council of Foreign Relations that “data is the new natural resource” to highlight the onset of a new era of computing involving massive amounts of data to understand and make decisions.[19] For the true potential of this new era to see fruition, governments must allow the market place to remain flexible to the changes by enabling the free flow of data; promoting a risk-based approach to security and privacy; encourage the development of systems with privacy and security inherent in their design; and continuing to enable the creation of open standards necessary for interoperability of devices and networks.

Today, privacy regulations around the world affect how businesses handle, process, control, protect, store, and move information related to people. IoT will create much more of this information, putting even more pressure on proper handling of such information. With the additional complexities of configurations, architectures, and multiple devices and communications paths being used in IoT applications, there will be even more data storage and data usage scenarios to consider. This includes data held inside devices or intermediate computing systems that is stored or cached while in flight or in transit.

Data Use: Policy considerations on data use should depend on whether the context is B2C or B2B.

- B2C: Use of consumer data should be governed by existing privacy, consumer protection, and unfair commercial practices law. A need to create IoT-specific regulations on data use is premature.

- B2B: Data use rights between commercial parties should be governed by contractual relationships that are consistent with underlying requirements concerning, e.g., intellectual property rights, use of or access to any personal data, and regulatory restrictions that may be relevant. If consistency with applicable regulatory requirements is assured, data usage rights can be included in contractual vehicles and agreed by parties during negotiations. Mandating uniform rules to govern data usage in B2B is not workable, as data usage depends on the use case and type of data, including whether the data is confidential, of value to the owners, or requires secondary data use rights.

16. *How should the government address or respond to cybersecurity concerns about IoT?*

[19] https://www.ibm.com/ibm/ginni/pdf/G_Rometty_Council_of_Foreign_Relations_Remarks_as_prepared.pdf

As stated above, at this time, the government should not be focusing on establishing new regulations, instead it should be fostering a flexible model that allows innovation for both technology and security at the same time. The government should also continue to foster a community for cybersecurity information sharing, and work with the private sector to establish clearer guidelines for appropriate security research and coordinated disclosure.

a). What are the cybersecurity concerns raised specifically by IoT? How are they different from other cybersecurity concerns?

Cybersecurity concerns apply to IoT much as they do to other digital environments. Connected devices can be used as personal devices as well as part of critical infrastructure. Most of the cloud-based IoT platforms as well as consumer-oriented devices may be managed in similar ways as we do today with cloud security and mobile phone security. However, there may be some cases where limitation arise from the embedded nature of the IoT device (as opposed to its platform), i.e., IoT devices may be constrained in processing capacity, memory capacity, available power, and lack of proximity to human interaction. This can limit the device's ability to be promptly updated, modified, and fixed after deployment and to defend and protect itself against attack.

Clearly this will vary as to the device itself and how it is deployed, and therefore the outcome of a cybersecurity attack may have very different results.

IoT may also combine both digital and physical systems that can directly affect safety – or can potentially cause harm to life or the environment. In all instances, cybersecurity protections should be included in hardened systems designed for resiliency and safety.

c). What role or actions 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?

The government should foster research and innovation in the area of cybersecurity in order to stay ahead of potential attacks and subversion. This is best done through open collaboration, information sharing, and competition in providing services to businesses to address this need. Examples of healthy collaboration and research exist with the NIST Cybersecurity Framework and CERT advisories.

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?

With IoT systems there is more data available, in more forms, and sampled closer to people (for example from wearable devices). As technologies for interpreting unstructured information advance, data collected by sensors may potentially be associated with individuals in new ways.

c). What role or actions 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?

Government should work to ensure the free flow of information, and recognize the global nature of the digital economy. Rights to and use of information should be handled through contractual terms and existing laws and principles, allowing for innovation and competition to occur and the market to determine appropriate use and handling of personal information. Government should promote "privacy by design."

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?

Many existing standards and guidance organizations, world-wide, are working on guidelines and recommendations for IoT and security in IoT systems. In particular, ISO/IEC, IEEE, ETSI, Industrial Internet Consortium (IIC), Open Interconnect Consortium (OIC), NIST, and CERT are working in this area as is the EU Alliance for Internet of Things Innovation (AIOTI).

IBM recommends a formal dialogue between the U.S. and other governments, including the EU, on matters related to IoT, including standards and regulations. By way of example, governments in both the U.S. and EU are currently in the beginning phase of developing a detailed IoT strategy. Therefore, these governments now have a unique opportunity to develop common approaches.

21. *What issues, if any, regarding IoT should the Department focus on through international engagement?*

We encourage the Department to recognize that for IoT's benefits to be fully enjoyed around the world, data must be able to flow across geo-political boundaries. Also, IoT will rely on network neutrality to ensure the IoT data will be able to move freely through communications networks. Other forms of connectivity between people and communities are diverging from geo-political boundaries. Examples of this are transportation, communications, water, and power networks. We encourage continued attention to network neutrality.

Cooperation among nations could also help develop:

- Rules for digital trade that enable data flows and limit data localization (for example, the Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) recognize that the ability to exchange information across country borders is a fundamental tool for business in the global digital economy; the APEC CBPR enable strong but trusted data flows in the APEC region that, by design, create more interoperability among varied governmental regulation);

- Synergies and interoperability in approaches towards cloud computing, cybersecurity, and encryption;
- Regulatory cooperation and standardization in Industrial Control Technology (ICT) products/solutions;
- Develop interoperable approaches to the Internet of Things (e.g., platforms, standards, data ownership, and reference architectures) and its use cases (e.g., healthcare, connected vehicles, smart manufacturing);
- Develop frameworks to promote transatlantic investment in research and development

23. *Are there policies that the government should seek to promote with international partners that would be helpful in the IoT context?*

With the rise in the number of devices simultaneously accessing and communicating over the Internet, continued attention to adoption of IPv6 is recommended. Further, government should encourage the adoption of wireless communications technologies which offer greater bandwidth and wider coverage. This extends both in the network speed dimension as well as the network coverage (e.g. low power, long range wireless networking).

Government should continue to promote and facilitate adoption of IPv6 over IPv4. IPv6 offers:

- longer address space than IPv4 to accommodate more devices being directly addressable on the network
- enables devices to have multiple addresses
- supports multicast, anycast, and other features
- better support for secure communications than IPv4

24. *What factors can impede the growth of the IoT outside the U.S. (e.g., data or service localization requirements or other barriers to trade), or otherwise constrain the ability of U.S. companies to provide those services on a global basis? How can the government help to alleviate these factors?*

Difference, or even worse contradictions, in IoT rules developed in other geographies will harm the ability of U.S. companies to export their IoT solutions because adjustments will be required resulting in additional cost, and in a lower competitive position for U.S. companies. Therefore, we strongly recommend the U.S. government to engage in international cooperation to develop common, or at minimum, interoperable rules.

Data privacy and localization regulations which are tied to geo-political borders are not in sync with how information and processing occurs by companies that serve a global customer set. It is important for global companies to be able to innovate and compete.

Allowing cross border data flows while balancing privacy and security obligations enables this innovation and competition. Overly restrictive regulations may result in stifling innovation and unworkable business constraints, resulting in lost business opportunities.

25. *Are there IoT policy areas that could be appropriate for multistakeholder engagement, similar to the NTIA-run processes on privacy and cybersecurity?*

IoT, by bringing together cyber and physical systems, will necessarily require the coordination and interaction between what have been separate areas of concentration in government offices. Some examples for the Department to consider include: FDA and NHTSA, as driver safety is affected by medical devices communicating with vehicles; FDA and OSHA, as worker safety is affected by wearable devices used by employees for worker safety and assist in reporting accidents and diagnosing medical problems; FAA and NTSB as a wider and wider range of autonomous, semi-autonomous, and large and small aircraft are used for business purposes.

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?

We recommend that an open and competitive market be used to find the appropriate use of IoT for enabling improved operations, lowering costs of operation, and facilitating better conservation of the environment. The Department of Commerce can ensure that such an open market continues to exist for the U.S. economy as more and more industries utilize the Internet and connected devices.

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?*

We recommend that government and the private sector continue to work together through open standards, research and development, and world-wide communications and agreement on regulations governing IoT. Government should foster innovation and competition by industry to design, implement, and deliver ever more available, resilient, and defensive (resilient, robust, resistant, and recovering) from attack, misuse, tampering, and malfunction. This is an area where fostering competition through research and contests could assist in advancing technology.

As with other digital environments in the past, IoT has a world-wide impact and influence, necessitating a global view to foster innovation and competition. A key component to realize this potential is “educating the next generation to participate in and contribute to the global digital economy…education has not kept pace with innovation, and disparities between children from low-income families in educational attainment and subsequent employment are greater than ever."[20] More should be done to prepare students with the kinds of technical, physical science and business skills that the labor market increasingly demands. Programs like P-TECH[21] and FIRST[22] are providing the environment and tools to help children thrive in science, technology, engineering and math (STEM) and chart a course for their educational and career paths. Government partnership and sponsorship of such programs are imperative to sustaining US economic competitiveness and growth of global economy.

C. Conclusion

The Internet of Things is revolutionizing the way we live by transforming everyday objects around us into an ecosystem of information and automation. From home security to smart refrigerators, everything is becoming more technologically advanced. The Internet of Things promises to connect the whole world into one huge information exchange.[23] IoT applications share information with us about the cars we drive, the tools we use, the buildings we live in, and the world around us. But without the addition of cognitive computing, the usefulness of the plethora of information now available would be limited by its own complexity and scale. We would only be able to see slivers of insight. The rest would remain in the dark. IBM believes that cognitive computing is fundamental in realizing the true value of the Internet of Things.

We emphasize the importance of adopting a "wait-and-see" approach before the promulgation of any new regulations that IoT would be subject to. Interagency and international coordination between the U.S. and other governments, for example the member countries of the EU, is essential in crafting a legal framework that not only achieves its regulatory goals but continues to foster innovation and competition. By encouraging innovation and competition, the government should encourage the IoT market to build security and privacy by design, and to promote trust and confidence in developing and implementing IoT. Promoting open standards and use of open source tools and capabilities encourages transparency and more inclusive participation of citizens and companies in the IoT ecosystem.

As with all evolving areas, flexibility is necessary to facilitate transformation. Similar to the approach taken to the development of the Internet, the details of the implementation of IoT and cognitive computing should not be mandated. IoT has the amazing opportunity to improve lives, streamline services and conserve resources, and can be best fostered by the government through a measured approach that prioritizes safety, accelerates adoption, drives competition, and encourages innovation.

[20] To Innovate, We Must Educate, blog post, Stanley S. Litow, VP, Corporate Citizenship & Corporate Affairs, January 20, 2016, http://www.huffingtonpost.com/stanley-s-litow/to-innovate-we-must-educate_b_9012094.html

[21] http://ptechnyc.org/

[22] http://www.firstchampionship.org/

[23] PTech@Brooklyn students describe "Internet of Things" https://www.youtube.com/watch?v=faB6lT0Uqhw

IBM appreciates the opportunity to provide this response and hope it will be helpful to the Department of Commerce in framing its analysis of IoT. We look forward to future collaboration with the Department on these important issues.

Sincerely,

Christopher O’Connor
General Manager, Internet of Things Offerings
IBM