DoIT
Illinois Department of
Innovation & Technology

Bruce Rauner, Governor

Hardik V. Bhatt, Secretary Designate & State CIO

The Honorable Lawrence Strickling
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Washington, DC 20230

May 23, 2016

Dear Assistant Secretary Strickling,

Please find attached State of Illinois comments in response to the National Telecommunications and Information Administration (NTIA) Request for Comments (RFC) on the benefits, challenges and potential roles for the government in fostering the advancement of the Internet of Things.

We commend the NTIA in issuing this RFC on this important topic. We believe the federal government has a critical role to play in the advancement of the Internet of Things in the US that will help citizens and businesses, especially start-ups, fostering tremendous economic growth while keeping cybersecurity at the forefront. It is imperative the US maintains its leadership in Internet technologies by developing a national strategy for the Internet of Things. While we do not recommend burdensome regulation, we do support the government in its role of facilitating research, policy, convening and federal agency implementation of Internet of Things solutions. We also recommend creating a Deputy CTO position at the White House that oversees all IoT related efforts within the Federal Government and interactions with the private sector.

The State of Illinois is undergoing a transformation to a Smart State, a transformation driven by communications and information technology with Internet of Things and Data analytics being key components. We welcome the opportunity to contribute on this topic as a thought leader and a practitioner. Please don't hesitate to contact me if you have any questions on our response.

Sincerely,

HVBhatt

Hardik Bhatt
Secretary Designate, Department of Innovation & Technology
State CIO, Office of the Governor, Bruce Rauner
State of Illinois
217 524 7083 hardik.bhatt@illinois.gov

Name of Filing Party: State of Illinois
Date: May 23, 2016

Before the
National Telecommunications and Information Administration
Washington, D.C. 20230

In the Matter of	**)**	
	)	
The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things	**)**	Docket No. 160331306-6306-01
	)	
	)	
	)	

COMMENTS OF THE STATE OF ILLINOIS REGARDING THE BENEFITS, CHALLENGES, AND POTENTIAL ROLES FOR THE GOVERNMENT IN FOSTERING THE ADVANCEMENT OF THE INTERNET OF THINGS

Date: May 23, 2016

The State of Illinois submits the following comments in response to the National Telecommunications and Information Administration Request for Comments on the Benefits, Challenges and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

Name of Filing Party: State of Illinois
Date: May 23, 2016

Table of Contents

Name of Filing Party: State of Illinois
Date: May 23, 2016

Introduction

The State of Illinois welcomes this opportunity to respond to the Request for Comments issued by the National Telecommunications and Information Administration to explore the benefits, challenges and potential roles for the Government in fostering the advancement of the Internet of Things.

We believe it is critical that the US leads the world in Internet of Things technology and implementation, driving economic growth and enhancing public safety, transportation, health outcomes, environment and better use of scarce resources. A national strategy for the US for Internet of Things is imperative to maintain our leadership in Internet technologies.

Led by Governor Bruce Rauner and Secretary of Innovation & Technology Hardik Bhatt, Illinois is in the midst of a transformation to a Smart State, we believe the first in the nation. We are in year 2 of a 4 year journey and we have much work to do. However, our learning, experience and expectations for the future guide this response and our recommendations.

Per the IDC White Paper that explains the Smart State and the transformation of Illinois into a Smart State (available at http://www.illinois.gov/sites/cio/Initiatives/Pages/SmarterIllinois.aspx), a Smart State is a state with a vision, a plan, and an execution road map to enact the digital transformation of government by investing in information and communications technology (ICT). This includes mobile technologies, big data analytics, social networks, and cloud services as its foundation for a set of innovation accelerators, such as the Internet of Things (IoT), cognitive computing, and robotics, that enable potentially radical new work processes, services, and products.

Illinois believes a Smart State has three roles that are relevant to this response and to a US Internet of Things National Strategy:

(i) **IoT for Government Efficiency**: Helping make government more efficient, effective and accessible by using information and communications technologies such as the Internet of Things and Big Data analytics. Driving better service to Illinois citizens and businesses, our customers.

(ii) **IoT for Economic Growth**: Supporting and facilitating entrepreneurship, innovation and investment in the Internet of Things industry, by improving policy and regulatory structure that fosters economic growth.

(iii) **IoT for Demand Aggregation (suburban and rural areas)**: Aggregating the demand by clustering of cities and regions allowing shared services and benefits of IoT to accrue to all towns and cities in Illinois. This should achieve cost savings for cities and regions and is particularly helpful for those rural areas that do not have the resources as well as enough demand to attract the private sector to deploy Smart City solutions.

We recommend the federal government include these three roles in its IoT strategy at a federal level. For example, the federal government itself can benefit enormously by the implementation of IoT applications, to increase efficiencies, effectiveness and accessibility of federal government agencies.

Regarding role (2) the federal government, for example via the National Science Foundation (NSF) and National Institute of Standards and Technology (NIST) and other federal agencies, is already facilitating research and thought leadership on the IoT and this is to be commended. Pushing for common open standards for IoT technology should ease adoption. Simplifying various policies and regulations focused on entrepreneurship will allow tremendous economic growth in this critical growth area.

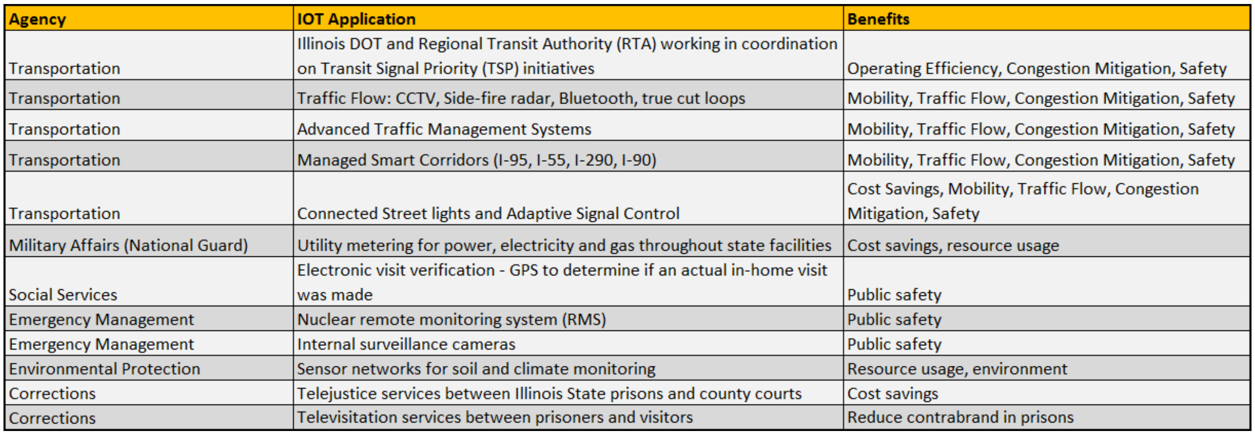
For role 3, within Illinois we will use the State broadband network, Illinois Century Network (www.illinois.net) (ICN), to support shared services between regions. This will enable equity in the deployment of IoT technology across all regions and enable shared services. The federal government should ensure that rural areas also benefit from the deployment of IoT technology, by facilitating and encouraging demand aggregation. Due to the very rural nature of Illinois this is of key importance to us.

We recommend that the Federal Government appoint a Deputy Chief Technology Officer in the White House Office of Science and Technology Policy (OSTP) – as Chief IoT Officer. The Chief IoT Officer should be responsible for coordinating across the Federal, State and local governments to enhance United States' position in all three areas (roles) as described above.

The following data points illustrate the unique nature of Illinois with large rural areas and concentrated population centers. The Chicago metro area has a population of approximately 74% (9.5 million) of the total population of Illinois (12.9 million). Another view is by City population. The City of Chicago has a population of approximately 2.7 million. The next most populous city is Aurora, with a population of approximately 200,000, with all remaining Illinois cities having populations less than 200,000. It should be noted that this population characteristic of Illinois effectively excluded all Illinois cities from the recent Department of Transportation (DOT) Smart City Challenge, which requested a "medium" sized city having a population of between 200,000 and 850,000 apply for available grants.

This population density characteristic of Illinois means we take very seriously role 3, the support of clustering of municipalities and regions. There are many small, rural towns in Illinois that do not have the resources to develop and implement smart city solutions. With a state wide high speed broadband network, we plan to alleviate and even eliminate these challenges. We recommend that the federal government address the challenge of implementing IoT in rural areas throughout the US, and recognize that it can help reduce the existing digital divide.

There is much industry interest in Internet of Things, with all manner of applications and use cases being posited. For Illinois State government there are real cost savings and real impact due to IoT. Impact along the lines of cost savings, public safety, transportation, energy usage and the environment. The below table provides IoT based applications that have been deployed or about to be deployed within Illinois. For each application we also describe the associated benefits.



Agency	IOT Application	Benefits
Transportation	Illinois DOT and Regional Transit Authority (RTA) working in coordination on Transit Signal Priority (TSP) initiatives	Operating Efficiency, Congestion Mitigation, Safety
Transportation	Traffic Flow: CCTV, Side-fire radar, Bluetooth, true cut loops	Mobility, Traffic Flow, Congestion Mitigation, Safety
Transportation	Advanced Traffic Management Systems	Mobility, Traffic Flow, Congestion Mitigation, Safety
Transportation	Managed Smart Corridors (I-95, I-55, I-290, I-90)	Mobility, Traffic Flow, Congestion Mitigation, Safety
Transportation	Connected Street lights and Adaptive Signal Control	Cost Savings, Mobility, Traffic Flow, Congestion Mitigation, Safety
Military Affairs (National Guard)	Utility metering for power, electricity and gas throughout state facilities	Cost savings, resource usage
Social Services	Electronic visit verification - GPS to determine if an actual in-home visit was made	Public safety
Emergency Management	Nuclear remote monitoring system (RMS)	Public safety
Emergency Management	Internal surveillance cameras	Public safety
Environmental Protection	Sensor networks for soil and climate monitoring	Resource usage, environment
Corrections	Telejustice services between Illinois State prisons and county courts	Cost savings
Corrections	Televisitation services between prisoners and visitors	Reduce contrabrand in prisons

Data

Special focus needs to be directed to data, including data governance, ensuring high quality data, having open data and promoting research in data analysis and analytics. We recommend the federal government take specific actions related to data that will improve outcomes for all citizens and recommend the federal government treat data with the utmost importance across all agencies.

With high quality data, provided by devices within the Internet of Things, we now have a much clearer, sharper view of the world. We can observe the world in much finer detail and act on that data with precision.

How we treat data has significant impact on the benefits that accrue from Internet of Things. Having privacy policies that respect an individual's right to privacy, but still enabling open data to the public, will promote advances in our knowledge and enable us to improve outcomes for the benefit of all citizens.

Data is a high priority in Illinois, and for this reason we are establishing a Data practice, led by a Chief Data Officer reporting to the State CIO. This practice will support big data management and governance, data analytics and will address issues of data privacy and security. The data practice will serve as a source of expertise for all State agencies, and a liaison with Federal parties as necessary.

The City of Chicago has developed an Open Data platform that provides a model for other states and nations. The platform, called OpenGrid, provides a platform to make data sets both machine and human readable and thus supports the further analysis of the data. OpenGrid operates on the Plenario platform with Plenario being funded by a National Science Foundation grant. More information can be found at (www.opengrid.io and www.plenar.io).

We encourage the federal government to ensure data is Open, to make available data sets, and encourage research in Big Data analytics by continuing to fund innovative big data projects, such as Plenario.

Conclusion

This section introduced the approach Illinois is taking to implement IoT. We are in year 2 of a 4-year transformation journey that began in January 2015. We have Chicago, the 3rd largest city in the United States, which is a great target city with its population density and scale for the IoT industry to grow. We also have a vast rural area that can benefit from IoT through sustained efforts of its Government by demand aggregation and pro-growth policy and regulations. We are using IoT to address real problems of the State to improve the quality of life for citizens, improve the environment and improve the Illinois economy. As well as transforming Illinois State government, we are focused on facilitating the implementation of Smart Cities throughout Illinois and ensuring the right regulatory, policy and legal framework exists. We are supporting the clustering of towns and cities, ensuring all regions in Illinois benefit from IoT and thus ensuring equity in the use of IoT. Our learnings guide our response, and we look forward to the publication of the Green Paper.

State of Illinois Responses to Questions

General:

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?

IoT is a disruptive technology that encompasses devices, cloud technologies, data, analytics and communication. While IoT can be considered an evolution of the Internet, the complexity IoT provides is a step function beyond what we have dealt with in the past. In the coming years, we can expect to see the number of connected devices increasing exponentially, with the devices literally being everywhere and all interconnected. Technological challenges we expect to see relate to:

- Security
- Big Data management and governance
- Interoperability
- Standardization
- Network management and administration
- Talent

Security. With the large number of interconnected devices, the security threat profile is raised significantly. Ensuring a secure network becomes both more critical and more challenging. Challenging due to the large number of potential access points in an IoT application and critical due to the important functions IoT applications implement.

In IoT applications, devices can communicate over multiple methods, from wired to wireless, with wireless including Near Field Communication to Fourth Generation Long Term Evolution (4G LTE). The connectivity and ease of information sharing between devices opens up many opportunities and challenges. For example, much of the connectivity can occur without a person's knowledge or consent. The challenge is to have a known source of connectivity (SOC) and for the device, user, person, sensor et al. to be "smart" so that it can still protect information sharing as appropriate. "Known source of truth" is also necessary to ensure approved connectivity and information sharing and avoid spoofing and Cyberattacks.

Big Data Management and Governance. With the proliferation of devices, in all form factors, and having immense processing power, we expect the quantity of data generated by the devices will be large, requiring big data management and governance procedures to be in place. With the IoT, information is generated predominantly by devices, versus people, as has traditionally been the case with the Internet. With the expected quantity of data produced and transmitted, categorizing data, managing the data, and respecting associated privacy and security requirements for the data will be a challenge.

Interoperability and Standardization. As we are in the early stages of IoT implementations, we are acutely aware of the issue of interoperability and standardization. Interoperability is an issue since we do not want to purchase devices, only to have them be obsolete within a few years due to non-interoperability with other devices, the cloud or data infrastructure. Standardization is a related topic that encourages interoperability. Actions that can accelerate standardization will also accelerate the benefits of IoT. For example, a role the Federal government can play is convening experts to facilitate faster standardization.

Talent. The level of expertise required to effectively implement IoT projects is high. IoT applications require expertise in not just broadband, but devices, sensors, cloud and analytics. The IoT requires highly trained technologically aware people to implement. The support of science, technology, engineering and math (STEM) training and initiatives to foster an increased number of high technology workers is needed.. We expect it to be challenging to recruit highly trained people verse in IoT technologies.

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?

Policy challenges presented by the introduction of IoT relate to

- Privacy
- Data management and data governance
- Security
- Liability

The challenges are novel due to the quantity and granularity of data connections, and the breadth of data flows. Being able to use analytics and computing power to detect trends between data sets and to determine personally identifiable information from a combination of data sets adds a new dimension to the policy landscape. Being able to use data to direct devices to autonomously act on the world and/or to receive information provides a plethora of scenarios that our current policies when written were not imagined. Even today, law makers, regulators and state and federal agencies are playing catch-up to IoT applications currently being implemented. As we look to policies addressing privacy, data management and governance, security and liability, we should think in terms of principles and fundamental approaches for IoT that are independent of the specific application. Tying policies to specific IoT applications is a losing proposition and this approach will always be playing catchup.

We have found in Illinois, existing policies and regulations provide a starting point but do not address the full set of possible scenarios. We are working to update our policies in a cross agency manner. Current policies in Illinois were written when the power of IoT was not understood or known.

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

The economic benefits could be enormous. As systems become more and more automated, there are huge efficiencies to be gained by individual automated systems being able to communicate and coordinate their activities. For example, manufacturing systems could automatically restock for the next production run, and then coordinate with transportation systems to deliver the finished products. Another area would be vehicle maintenance, a fleet could be interconnected, and self-driving trucks could be routed to the nearest maintenance facility as they come due for maintenance. Safety is another area that would benefit, hazardous materials manufacturing and transportation could be monitored in real-time, and problems could potentially be mitigated with coordinated automated systems.

Additional benefits to specific IoT applications being implemented in Illinois are seen in the Table on page 4. We also see and expect to see IoT benefits in the following categories:

- cost savings
- enhanced public safety
- better health outcomes
- better environmental monitoring
- enhanced building management
- transportation – enhanced traffic flows, increased 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. 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?

Illinois takes an expansive view of the definition of the IoT, which should help to devise appropriate policies and regulations for IoT deployment. An expansive definition allows consideration of all policy questions, and helps keep regulations in line with technology development. A limited definition of IoT would provide a small lens for introduction of policy, laws and regulations.

We want any policies or laws and regulations enacted to remain in place and be relevant for the long term. The fear of having too narrow a definition of IoT is that policy and regulation is soon outdated. We need to recognize the high rate of technology advancement in this arena.

IoT includes the combination of devices, cloud computing, data, analytics and broadband to monitor, control and affect external sources and the external environment. For this definition we assume the following extrapolations:

- Each device has unlimited processing power, or whatever processing power is needed to perform the task
- Each device has unlimited bandwidth capability (for information transfer), or the bandwidth required to perform the task
- Each device has unlimited memory / storage capacity, or the memory / storage capacity required to perform the task
- A device can be any shape or size
- The device has whatever sensors and / or transducers are required to receive information and enable positive outcomes. The sensor is used to receive information and the transducer is used to enable the positive outcome. There is no limit to the capability of the sensors or the transducers on the device.
- Data can be used by any device as necessary for the task
- Data follows a person and / or device as necessary for the task
- Access to relevant data by devices is seamless
- Data that needs to be protected and secure is protected and secure

By thinking of IoT in an expansive manner and thinking about IoT with these extrapolations, we can better provide policies, regulations and/or laws that support the development of IoT in Illinois over the coming years. The applications people dream up with IoT will be wide ranging, diverse and novel. Introducing policy, regulations and laws that is cognizant of the rapid technological change will help to support the new applications being created.

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?

General guidance and information exists in the industry, but the goal should be to draft a comprehensive policy that can be reviewed and agreed to by the industry. For example, the City of Chicago are soon to release a privacy and data governance policy document, that was initiated in part by the Array of Things project, and the privacy concerns raised. The Array of Things project is a NSF funded IoT collaboration between Argonne National Laboratory, University of Chicago and City of Chicago. The project will place 500 sensor devices throughout Chicago to measure real time data on the city environment and infrastructure. It is like a fitness tracker for the City. More details can be found at https://arrayofthings.github.io/.

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

In Illinois as we think about policies, regulation and laws governing the IOT we are mindful of not introducing policies, regulation or laws that are too burdensome.

For example, with respect to Data, we have an Open Data policy, where data, without Personally Identifiable Information (PII) is made public, to be machine and human readable.

We are mindful of the unique geography of Illinois and will work to ensure policies for IOT provide equity in the deployment of IOT throughout Illinois, for both urban customers and rural customers.

We encourage the government to ensure that regulations are not burdensome and there is equity between rural and urban areas.

4. Are there ways to divide or classify the IoT landscape to improve the precision 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.

The classifications suggested in the question we agree with, thus classifications we recommend are:

- Public vs. private
- Within private consumer vs. industrial

Within the above two classifications, we can further define the IoT landscape to be:

- Person to device
- Device to device

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?

The Array of Things project in Chicago provided the impetus to develop a privacy policy and a data governance and management policy. This policy framework allows to further introduce IoT applications that align with the policy. The document is expected to be released during 2Q 2016.

Devices are becoming un-seeable such as the passive RFID technology that is being used in many industries including healthcare. We can expect to see IoT medications that can be swallowed.

Some areas will need more regulation than others…as alternative currencies including Bitcoin and Blockchain become a viable alternative to currency exchange Financial Services will require a higher level of regulation. In addition Public Safety needs to be a protected and secured spectrum and Healthcare needs to be protected to the utmost.

We recommend that a broad policy be developed but specific guidelines are provided for Financial Services, Health and Wellness and Public Safety.

Technology:

Technology is at the heart of IoT and its applications. IoT development is being driven by a very diverse set of stakeholders whose expertise in science, research, development, deployment, measurements and standards are enabling rapid advances in technologies for IoT. It is important to understand what technological hurdles still exist, or may arise, in the development and deployment of IoT, and if the government can play a role in mitigating these hurdles.

6. What technological issues may hinder the development of IoT, if any?

a. Examples of possible technical issues could include:

i. Interoperability

ii. Insufficient/contradictory/proprietary standards/platforms

Key technical issues that we see potentially hindering the development of IoT are security, interoperability and standardization in that order. IoT applications increase the importance of security and provide a challenging environment to maintain security. The devices provide potential access points for a security breach. The network itself must also be secure. The level of security attack prevention required increases exponentially with the corresponding increase in devices.

Maintaining network-wide security is vital, especially as we move the operations of critical infrastructure to the Iot, and especially as automation takes hold. In this scenario, a network breach is not a simple matter of losing money through banking fraud, but it becomes an enormous public safety issue. We are already at the point where there are deep concerns about the safety & security of the networks controlling the electrical grid, power plants, water treatment plants, and the like. Consider, for example, when self-driving vehicles, or self-driving construction equipment becomes a reality. At this point, security becomes a real safety issue, simply consider the damage that could be done if criminals or terrorists are able to take control of a self-driving tractor-trailer, an automated bulldozer, or an automated cargo aircraft.

With the quantity, type and breadth of data available or soon to become available, it becomes ever more important to secure the network and protect against security breaches.

Interoperability and the related standardization are key issues as IoT applications develop. It is important that devices are not made obsolete as standards evolve or interfaces develop. We recommend supporting and facilitating the standardization process for IoT applications.

The thousands of devices that will exist in the IoT infrastructure need to communicate and provide data, to be analyzed and acted upon. To enable interoperability, standards for data transfer and control need to be worked on.

iii. Spectrum availability and potential congestion/interference

Radio Frequency (RF) Interference will be an enormous problem that will be generated by IoT. It is reasonable to expect that of the billions and billions of devices that would be expected to be deployed, a substantial proportion will use RF in some form i.e., WiFi, Cellular, or other RF method, to communicate into the overall network. Even with properly designed and produced RF equipment, the sheer number of devices, potentially millions of devices in an urban area for example, will generate harmful interference that will be detrimental to the spectrum in that area. Not only is there the potential for IoT devices to interfere with themselves, a larger problem is the potential of interference to other users of the overall spectrum.

A short explanation may be helpful: any RF transmitter generates not only the desired signal, but also undesired signals. Even the most well designed and built transmitter generates a miniscule amount of interference of some type. An individual device, on its own, usually does not affect other users of the spectrum. However, if we begin to add millions of transmitters, each contributing a miniscule amount of interference, the cumulative effect will be a substantial amount of interference to the spectrum in that area. The effect is like comparing two people having a quiet conversation in an auditorium to tens of thousands of people attempting to hold a conversation. As more and more people are talking, the background noise level rises with each added conversation. At a given point it becomes very difficult for anyone to have a conversation.

iv. Availability of network infrastructure

Not only will the physical availability of the network (connection points) be critical, and in short supply in rural and wilderness areas, but the amount of network capacity will be severely strained by the IoT. The amount of data generated by billions of devices, especially considering that video may be a large component, will overwhelm current networks just due to the sheer amount.

v. Other

Malfunctions and Repair, at some point in the operation of every network or system, malfunctions will occur. Generally, the more complex the system is, the failure mechanisms will become more complicated, especially if it is in software/firmware. Even though the individual failure is usually very simple, the symptoms can be very misleading, and finding that individual failure can be very challenging. IoT will be the most complicated system created by humans so far, the concern will be if human beings are able to properly troubleshoot, repair, and monitor a network of this size and complexity. As an example, a malfunctioning device on one side of the world could cause an actual failure on the other side of the world. And this could occur even if there is no actual malfunction, just a difference in configuration and implementation that is not compatible. Resolving this type of situation will be extremely complex.

b. What can the government do, if anything, to help mitigate these technical issues? Where may government/private sector partnership be beneficial?

To help mitigate these technical issues, we recommend the government do the following:

- Support research in security and big data
- Convene stakeholders to address interoperability and standardization issues
- Support establishment of common policy and guidelines as relates to security, privacy, data governance
- Through the IoT implementation in federal agencies, facilitate security, interoperability and standardization. Federal agency Request for Proposals (RFPs) can encourage vendors to align with interoperability and standardization requirements
- Support Innovation accelerators and test bed environments – please see below for more detail

"Innovation accelerators" are entities which can move basic to applied research to create solutions for the marketplace. Organizations that apply a consortium approach to bring together expertise and leadership from across academia, industry and startups to research, develop, and test solutions will be most successful in addressing the type of industrial challenges and opportunities IoT enables. No one sector or player can address IoT challenges and opportunities on its own; the government should look to expert conveners and facilitators to define key problems and build cross-sector solutions.

Testbed environments are where cross-sector collaborations can demonstrate and apply learnings. In addition to further fueling innovation and collaboration, these types of environments can also serve training and student instruction purposes. Workforce development training in industry areas such as cybersecurity and manufacturing will require these physical facilities.

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?

Priority of technical activities with regards to IoT should be prioritized as:

- Security
    - We believe security is the highest priority technical challenge with the Internet of Things. The consequences of a security breach in an IoT implementation has the potential to be widespread and very damaging. The increase in available access points and the proliferation of devices provides a target for hackers and malicious entities that seek to do harm. Facilitating a baseline of high security, minimizing the level of human interaction needed to achieve the high security, is research we support
- Interoperability
    - Device and infrastructure interoperability is necessary for the survival of the IoT ecosystem. Developing standards will lower the barriers to entry for vendors and

promote competition. We do not want key interfaces or functionality to be controlled in a monopolistic manner. We want a vibrant ecosystem of IoT devices to be developed.

- Big Data governance and analysis
    - As described in the introduction of this response, we view Data as a key resource in IoT, and it is data, and the ability to glean information from data that provides tremendous benefit from IoT applications. It is data that is the source of the actions IoT devices take. Data and the ability to capture data in a granular manner and the ability to control devices in a fine tuned way provide the tremendous benefit to IoT. We support continued research in Big Data, Big Data analytics and the interaction between Big Data and IoT.
- Shared services
    - Much of Illinois is rural. We want to ensure the benefits of IoT accrue to not just the principal cities but to all regions, including rural areas. Many towns in Illinois do not have the resources to develop complete IoT or Smart City infrastructure thus we believe it is necessary to enable shared services between cities and towns. Research into the implementation of IoT shared services is supported and welcome. We want to ensure all Illinois benefits at the same pace by leveraging expertise developed in specific cities. We expect a high speed broadband network to facilitate shared services and in Illinois we are ready to utilize the state broadband network for the benefit of all Illinois.
- Fundamental Infrastructure Development
    - This means supporting development of the key building blocks of IoT and ensuring the US maintains its lead in this technology. For example, supporting research regarding device form factor, device processing power, cloud computing, broadband networks, big data flows and data analytics and their interaction will ensure we maintain leadership

Infrastructure:

Infrastructure investment, innovation, and resiliency (such as across the information technology, communications, and energy sectors) will provide a foundation for the rapid growth of IoT services.

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

As industry areas such as smart cities and digital manufacturing that rely on IoT continue to grow, new types of infrastructure and ways of linking old infrastructure are being created which will require a thoughtful approach to stability and security. Within cities, a growing number of points within buildings, roadways, electrical networks, water and sewage pipelines, and waterways are connected. The connected built environment further increases reliance on devices and platforms, as city officials use this data to derive insights and make operational decisions. Likewise, IoT within digital manufacturing simultaneously unlocks more data and new efficiencies while also creating more points for insecurity.

Another key issue is the explosion of the amount of data collected and who it is collected by. A common policy and approach to big data will be needed.

We believe IoT will exercise security and capacity of existing infrastructure. IoT implementations utilizing existing broadband networks will rely on the security capabilities of the underlying network. With the additional access points due to the IoT devices, we will need to ensure a highly secure network

Capacity of the network will be taxed due to the potential for significant data flows. Although many data flows will be low bandwidth, the potential combination of devices could result in large and numerous data flows.

Another demand on the infrastructure is due to the proliferation of many devices on the infrastructure. We could have potentially thousands of sensor devices, each with very small form factors, sending large quantities of data to a cloud service.

Each implementation of an IoT device will require an incremental addition to the infrastructure for support. For example, each device will need:

- Power, either wired or alternative like solar, requiring the production of solar power systems or the production and installation of copper wire, and other commodities
- Network access, either wired or wireless, again, this will require some sort of cable connection to be installed, and/or the use of increasingly crowded spectrum.

All the benefits of IoT in supporting our economy and society will be offset by the need to use resources to support the network. In some cases, IoT has the potential to put strain on supply chains, commodity supplies, spectrum , and other sources of support.

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?

Redundancy within the network and establishing a two or three factor authentication model for connected and completing transactions should be considered. Also known source of truth needs to be established. This will address the question ‘Is this a trusted connection’?

Ensuring security is addressed and handled appropriately will also ensure IoT disruptions are minimized.

10. What role might the government play in bolstering and protecting the availability and resiliency of these infrastructures to support IoT?

We recommend the following roles for the government:

- Convening role for security, and how to address security in the current implementations. (This is the biggest issue we have with implementing IoT in current architectures.)
- Work with industry to establish common strategies and guidelines around connectivity, known source of truth, data capture and storage, network resiliency and create “rules of the road” for vendors and solutions in the IoT space
- Provide data interoperability guidance
- Support a device and network agnostic approach to enable IoT innovation

- Support research, convening, federal agency implementations for security, capacity and resiliency

Economy:

IoT has already begun to alter the U.S. economy by enabling the development of innovative consumer products and entirely new economic sectors, enhancing a variety of existing products and services, and facilitating new manufacturing and delivery systems. In light of this, how should we think of and assess IoT and its effects*?* The questions below are an effort to understand both the potential economic implications of IoT for the U.S. economy, as well as how to quantify and analyze the economic impact of IoT in the future. The Department is interested in both the likely implications of IoT on the U.S. economy and society, as well as the tools that could be used to quantify that impact.

Page 4 of this paper provides a table of existing Illinois IoT Initiatives and benefits. Integrating IoT into our Illinois economy is still in the preliminary stages and we will develop metrics as we identify opportunities.

Measuring the impact of IoT both in Illinois and the nation will be visible mostly through economic statistics. Industrial production and service productivity figures should increase slowly over time, with a gradual decrease in unskilled employment openings, with an increase in highly skilled jobs continuing the trend of the last twenty years. GDP per person will also rise through demand for new services, products and new efficiencies. Individual metrics like kilowatts per hour used by individuals and entities, water usage per capita and petroleum/natural gas usage per capita should all decline relative to output, due to decreased waste and more efficient usage. Crop yields analyzed per inputs should rise, as soil, fertilizer and water management will be affected positively through IoT. In logistics and transportation, selected average delivery and commute times should decrease as sensors in streets and vehicles can calculate more efficient routes. Border and port container inspections can be automated using IoT sensors. In health care, nursing home & end of life care will become more efficient as patients can be monitored at home through telemedicine and remote health monitoring. Monitoring big data transfers and usage can also be tied into the effectiveness and usage of IoT. The more data we use on IoT, there should be a correlation and trend toward greater efficiency.

11. Should the government quantify and measure the IoT sector? If so, how?

The impact of IoT should be quantified, measured, and analyzed. IoT will have various effects on the economy and especially the quality of life for our citizens. These effects may or may not be readily apparent, measurement and analysis is the only way to know what the actual effects are and will give us a baseline for making changes to policy or technical issues.

a. As devices manufactured or sold (in value or volume)?

b. As industrial/manufacturing components?

c. As part of the digital economy?

i. In providing services

ii. In the commerce of digital goods

d. In enabling more advanced manufacturing and supply chains?

e. What other metrics would be useful, if any? What new data collection tools might be necessary, if any?

See above.

f. How might IoT fit within the existing industry classification systems? What new sector codes are necessary, if any?

12. Should the government measure the economic impact of IoT? If so, how?

a. Are there novel analytical tools that should be applied?

b. Does IoT create unique challenges for impact measurement?

13. What impact will the proliferation of IoT have on industrial practices, for example, advanced manufacturing, supply chains, or agriculture?

a. What will be the benefits, if any?

In manufacturing, IoT creates the opportunity for improved productivity in the production process and the supply chain. Processes require minimal oversight or human intervention; product specifications are automatically readjusted. Parts can be automatically resupplied.

Within cities, IoT has created an explosion of data that enables better and faster decision-making capabilities to guide and govern infrastructure use. It is possible to capitalize on opportunities to integrate data from public and private sources to revolutionize how citizens and organizations interact with the built environment and vice versa. From self-reporting buildings and roads to the optimization of public and private services, there are opportunities to guide interactivity with and within the built environment. For example, knowing when equipment or infrastructure might fail will drastically inform infrastructure upgrades, replacement, maintenance and corresponding capital planning.

Agriculture could especially benefit from IoT-linked machinery, the ability to use self-operating tractors, harvesters, etc., could revolutionize farming. Automated farm machinery, especially when linked to an infrastructure to supply, operate, and monitor their operations could operate with a speed, efficiency and precision not available today with human operators. We are seeing numerous applications of technology and partly-automated farming, however IoT could bring all these disparate pieces together into one overall system.

b. What will be the challenges, if any?

As mentioned in other responses, complexity, security, safety, and net job losses to human beings are primary challenges to IoT in any industry. But these challenges will become opportunities for software developers, as they develop products to ensure and enable a privacy wall between consumers, businesses and government institutions. More open data systems will be needed, as they promote security and efficiency and improve outcomes when we analyze public data. Availability to quality education is also a key component, which may need a major overhaul to keep the human component on equal terms to the rapid changes brought about by the IoT revolution.

c. What role or actions should the Department of Commerce and, more generally, the federal government take in response to these challenges, if any?

Government institutions can help IoT development by fostering environments for innovation and creativity by withholding regulation and taxes, along with providing economic incentives. At the same time they should monitor real time developments in the industry toward the goals of safeguarding individuals and organizations' privacy and identifying any potential public policy issues. And as mentioned above, major changes to the one hundred year old educational philosophy and structure need to be made in order to provide equal opportunities for the entire population.

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?

From a business perspective, this could be a very good development, as IoT has the potential to better control remote automated processes and used as a tool to supply goods and services could increase profits for most businesses.

However, for some workers directly, this could be a bad development. As more automation is used, the fewer actual human workers are needed. This could accelerate into a negative trend if one considers the possibility that if the workforce participation rate is driven to a very low rate, workers/consumers might end up with little to no money to spend. The question then becomes: "Who will purchase all the goods that have been produced through automation?"

This question of worker displacement becomes a fundamental issue, as it is not clear what types of jobs displaced workers could move to. Normally, we think of low-skilled workers as the ones who would be replaced, but as technology continues to advance, and the implementation of automation is accelerated by IoT, high-skilled professions could also be affected.

Creative destruction in economies has been happening for over 300 years, and it will be no different with the IoT revolution. What is needed by the government may be a substantial shift in educational policy, with focuses on STEM knowledge (specifically in Computer Science and Engineering). In order to spread this change throughout the whole state, learning clusters need to be defined through existing networks such as Community Colleges, libraries, chambers, city halls, SBDC centers, etc. All these institutions need to be accessed by broadband so information can be "pushed" both ways, to provider and user, therefore creating knowledge. The educational system should be changed, providing expedited pathways to STEM occupations, business, entrepreneurship, academia, services and manufacturing.

Policy Issues:

A growing dependence on embedded devices in all aspects of life raises questions about the confidentiality of personal data, the integrity of operations, and the availability and resiliency of critical services.

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

The main policy issues that affect or are affected by IoT relate to:

- Privacy,
- Data management and data governance,
- Security
- Liability

To advance these policy issues, we recommend the government:

- Advance thought leadership in these issues by convening expertise
- Research data categorization and privacy, and the impact of combining multiple data sets
- Provide a leadership role based on applications implemented for federal agencies to establish privacy, security and data governance policies

We do not recommend burdensome regulation or policy but rather a targeted approach to policy questions, that protect an individual's privacy, but still allows all parties the ability to advance the benefits drawn from the IoT.

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?

Cyber Security or Network Security will be a major factor in the safety and usability of IoT. Each of the potentially billions of devices connected to the IoT will present a security vulnerability. Much like a large building, all it takes is one unlocked door to breach security.

Maintaining network-wide security is vital, especially as we move the operations of critical infrastructure to the IoT and as automation takes hold. In this scenario, a network breach is not a simple matter of losing money through banking fraud, but it becomes an enormous public safety issue. We are already at the point where there are deep concerns about the safety & security of the networks controlling the electrical grid, power plants, water treatment plants, and the like. Consider, for example, when self-driving vehicles, or self-driving construction equipment becomes a reality. At this point, security becomes a real safety issue, simply consider the damage that could be done if criminals or terrorists are able to take control of a self-driving tractor-trailer, an automated bulldozer, or an automated cargo aircraft.

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)?

We recommend a standardized approach to Cyber Security across the classifications listed in Question 4, with additional emphasis on certain aspects based on the categorization. Protection from hacking is just as important to the industrial user as the home user wishing to guard their privacy from a breached network.

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?

This is an area where the development, requirements for use, and enforcement of standards is critical to enhance security as much as possible. Regarding policies, rules and/or standards regarding IoT cyber security, we recommend the government:

- Convene experts to advance security for the IoT
- Fund research in IoT security, that minimizes the level of human interaction required to enforce
- Through the IoT RFP's issued by federal agencies, specify security requirements

17. How should the government address or respond to privacy concerns about IoT?

To address privacy we need to appropriately categorize data. Once data is categorized, the data categorization governs its use. For example, an initial categorization would be if the data contains personally identifiable information (PII) or not.

It is recognized that it becomes harder to categorize data where PII is not in the data, but when processed and aggregated with other data sets PII becomes known. Perhaps there are levels of PII, where we obtain knowledge about a population group or an area, but that is not completely personally identifiable. It comes down to categorizing the data and then having associated rules and allowed actions on the data set. We want to have open data, and make data available to the general public, while respecting the privacy of citizens.

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

Privacy concerns raised by IoT are an order of magnitude more than privacy concerns we see today, for example, with the Internet. The principal difference is with the sheer size of the network and the number of connected devices. Based on device capability, there are many use cases that impact privacy. Devices having cameras and/or microphones provide an obvious impact to privacy. With the combination of tremendous processing power to analyze device input and make inferences privacy concerns abound. The issue is not just with personally identifiable information, but information that impacts population groups, or an area, could be considered an intrusion. Being able to derive personally identifiable information or even identifiable information (that is not personal, but associated with a group) from multiple data sets is another privacy concern.

As data holds personal information, the security of that data and the network supporting the data becomes ever more important. A security breach of the IoT, impacting both devices and data, becomes very impactful

b. Do these concerns change based on the categorization of IoT applications (*e.g.,* based on categories for Question 4, or consumer vs. industrial)?

At the fundamental level, privacy concerns remain the same across the IoT categorization, however, within each categorization, there are areas of emphasis.

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?

We believe a reasoned approach to privacy and the IoT is necessary, that strongly protects data containing personally identifiable information, but that also makes data sets that do not contain PII public and open. We want the privacy rights of entities in the IoT to be respected, but also want to maximize the potential benefits derived from IoT.

We do not want burdensome policies, rules and/or standards to inhibit IoT implementation and deployment.

18. Are there other consumer protection issues that are raised specifically by IoT? If so, what are they and how should the government respond to the concerns?

Privacy policies, procedures, rules and regulations as it pertains to IoT should be written in a manner that puts people first.

19. In what ways could IoT affect and be affected by questions of economic equity?

Potentially, IoT could aggravate economic inequity as it pertains to workforce automation. Employee costs are usually the single largest expense borne by any business. The pressure to cut employee costs is a strong one, and an interconnected network of automation that replaces human workers will drive costs down for employers. The drawback is that as automation replaces more and more workers in all ranges of skills, from low to high, it will be important to make sure that all those displaced workers are not simply cast off and abandoned. It is an entirely possible outcome of IoT that more and more wealth and resources are concentrated in a smaller and smaller group of people, making for increased discussion regarding income and wealth inequality.

a. In what ways could IoT potentially help disadvantaged communities or groups? Rural communities?

IoT has the potential to help rural communities access services previously only available to those in urban communities. IoT in healthcare, providing the ability to remotely monitor, can help bridge the geographic and economic gap that often exists between rural and urban communities. Being able to remotely control devices could allow healthcare to be provided locally. Other examples exist, where the ability for devices to monitor or control, enables rural communities to remain in place, and still have the full benefits as if they were living in an urban community. Disadvantaged communities benefit, when IoT provides a cost saving by device processing power increasing.

b. In what ways might IoT create obstacles for these communities or groups?

A lack of broadband would have a severe impact on the implementation of IoT in these communities. There is already a recognized lack of broadband in rural areas, and trying to implement IoT without adequate broadband will not result in a successful IoT project implementation.

What effects, if any, will Internet access have on IoT, and what effects, if any, will IoT have on Internet access?

A key component of IoT is communication, both wired and wireless. The lack of high speed broadband could serve to hinder deployment of IoT in a community. It becomes table stakes that a high speed broadband network is available for communication between IoT infrastructure.

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?

We recommend the support of shared services between regions to help both rural communities and disadvantaged communities. Providing support for scalable high speed broadband in rural communities is a necessary pre-requisite for the support of IoT technologies. Assisting rural communities adopt IoT with the implementation of “low hanging fruit” applications we support.

We should be careful to not only focus IoT implementations on cities with a certain population, but to understand that IoT can benefit all governmental entities, from federal government to state government to cities, towns and villages in the US. In Illinois, we are supporting the adoption of Smart City solutions to all regions of Illinois as well as the clustering of regions to ensure all communities benefit from Smart City deployments, thus IoT.

International Engagement:

As mentioned earlier, efforts have begun in foreign jurisdictions, standards organizations, and intergovernmental bodies to explore the potential of, and develop standards, specifications, and best practices for IoT. The Department is seeking input on how to best monitor and/or engage in various international fora as part of the government’s ongoing efforts to encourage innovation and growth of the digital economy.

20. What factors should the Department consider in its international engagement in:

a. Standards and specification organizations?

One thing to consider is that very often, technological development and application occur under the overall philosophy of the society where the technology is developed. In other words, when technology is developed in a culture where concepts such as privacy are not valued, the technology will be developed without the necessary safeguards. Any standards bodies that the US participates in will need to keep privacy and other concepts uppermost in their standards development. Also, it will be incumbent on the US representative to make sure the concepts that are important to the citizens of this country are included.

b. Bilateral and multilateral engagement?

c. Industry alliances?

d. Other?

The government should facilitate and support alliances and cooperation between regions in the US and across the world. Both regional and industrial alliances should be supported.

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

22. Are there Internet governance issues now or in the foreseeable future specific to IoT?

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

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?

Additional Issues:

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

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?

Providing case studies of IoT applications implemented in federal agencies thus far will be useful as will the support of master contracts.

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?

A national strategy that guides the nation to be the leading nation for IoT we believe is necessary and preferable to a completely hands off approach.

A strategy for digitization of key industry and/or sectors will fuel IoT growth and development. There are several frameworks for this strategy. The first is defining key IoT “ecosystems” such as urban data or digital manufacturing. The second is considering within those contexts the ways data is being collected, managed and used. In terms of collection, what are the devices and storage systems being utilized? In terms of management, how is data being aggregated from these IoT enabled devices and platforms, and how is it being secured? Finally, how is data being used to inform new markets, provide analytics and insights, or create new business models?

The government and private sector can work together to prioritize ecosystems with the highest potential for leveraging IoT, as well as the greatest need for managing risk. Viewed across the data ecosystem of initial collection via devices and sensors, management via platforms and storage, and use by public and private entities, new policy and regulatory recommendations can be produced to both mitigate risk and promote growth opportunities.

28. What are any additional relevant issues not raised above, and what role, if any, should the Department of Commerce and, more generally, the federal government play in addressing them?

--- End of Document ---