Comments of the

Secure ID Coalition

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"

81 Fed. Reg. 19956 (April 6, 2016)

Submitted to iotrfc2016@ntia.doc.gov
June 2, 2016

The Secure ID Coalition welcomes the opportunity to provide the U.S. Department of Commerce with information regarding the benefits and challenges posed by the growth of the Internet of Things (IoT), as well as the potential role of the government in fostering a robust IoT marketplace. The Department's announcement represents a bold step forward in laying the groundwork for an Internet of Things that fosters innovation, accelerates economic growth, and improves consumers' quality of life. Our comments will endeavor to assist the Department of Commerce to understand this need for a balanced regulatory approach. We also look forward to engaging in an ongoing dialog with the Department as technology innovations will shape and reshape the IoT landscape.

Founded in 2005, the Secure ID Coalition works with industry experts, public policy officials, and federal and state agency personnel to promote identity policy solutions that enable both security and privacy protections. Because of our commitment to citizen privacy rights and protections we advocate for technology solutions that enable individuals to make decision about the use of their own personal information. Members of the Secure ID Coalition subscribe to principles that include the increased deployment of secure identity solutions, as well as advise on and advocate for strong consumer privacy protections and enhanced security to reduce waste, fraud, theft and abuse. Our mission is to promote the understanding and appropriate use of technology to achieve enhanced security for ID management systems while maintaining user privacy.

Secure ID Coalition members are constantly solving technological challenges standing in the way of greater IoT adoption in areas such as computing power, interoperability, connectivity, and energy storage. Secure ID Coalition members are also developing and deploying the most advanced digital security technologies available assisting forward-thinking companies as they better use data to serve their customers. Their innovations are relied upon by consumers, private companies, and governments at every level across the United States to increase efficiency, manage complex enterprises, and make life easier.

When policymakers attempt to understand the Internet of Things as a concept, they should keep two foundational ideas in mind: First, Internet of Things devices and solutions incorporate a stunningly wide range of applications, including fitness trackers, healthcare devices, asset management, product tracking, and climate sensors, to name a few. While many of us tend to focus on devices we may carry on our person or install in our homes, a huge number of IoT devices work behind the scenes to facilitate

a wide range of essential industrial and commercial applications. Though these functions may be invisible to the end user, they are nonetheless critical to delivering the products and services we deem essential to our everyday lives in a data driven interconnected world.

Second, although there exists an immense variety of devices and solutions within the Internet of Things, most can be suitably categorized as either consumer or industrial applications, and it is useful for policymakers to keep this distinction in mind when considering regulatory proposals. Consumer applications contain interfaces that allow users to consciously interact with their devices; incorporate sensors that collect data from users or their environments; or transmit, analyze or store data generated via users or their environments. By contrast, industrial IoT applications exclude an end user that could serve as a frame of reference. These applications are increasingly necessary to manage the intricate business processes at the heart of the global economy and ensure the performance of complex systems and devices, however the data they collect rarely contains personally identifiable information (PII) that can be traced back to individuals acting in their capacities as consumers.

The most significant challenge confronting the Internet of Thing's continued growth involves security and privacy concerns related to data generated from consumer applications. Deploying security- and privacy-enhancing IoT technologies and solutions strategically and systematically in order to both keep user data secure and protect devices from malicious actors is the challenge before all manufacturers, corporations, and end users utilizing IoT technologies. Failure to do so would result in a serious breach of trust between consumers and the organizations seeking to deploy the technologies. It is no exaggeration to state that such a loss of trust would constitute an existential threat to the growth and widespread adoption of the Internet of Things. Simply put, without trust, the Internet of Things will remain an *innovation that could have been*.

While data security and integrity are paramount in all IoT environments, it is useful to consider a spectrum with consumer applications on one end and industrial applications on the other. Information gathered on the consumer end of the spectrum–in particular PII–must be afforded additional protections under a framework that stipulates who owns the data, what notice and consent rules will be observed, how the data will be stored, managed and used, and actions that will be taken in the event of a breach of that data. Negotiating the balance between user data that must be afforded additional protections and additional data (which may nonetheless be sensitive in its own right) will be an important challenge for policymakers moving forward.

Essential to understanding IoT's impact on daily life is recognizing how ***identity*** plays a relational role in the connected device's daily use. In the following categories of interactions—device-to-device, device-to-human, device-to-application/service, and human-to-application/service—all project their own identity information. Stakeholders must recognize the key role human identity plays in these processes, and deploy frameworks and technologies designed to protect those identities and the linked data.

Every object within the IoT realm produces data, and that data may lead to PII that might require heightened protection. For instance, a connected bathroom scale might relay body weight recordings via email to a number of people, including the family physician who records it as diagnostic health data in a patient's health record. This information may now be considered personal health information, protected under HIPAA. In order to properly handle this data, it becomes important to know *whose* data it is – and without having an identity verification layer in the connected device, a physician doesn't know if it belongs to mom, dad, the family dog, or a curious plumber fixing a clogged drain. As such, IoT device manufacturers and IoT service/application providers should be mindful of the potential harms to

consumers, as well as risks to data collectors, when proper identity verification is not incorporated in the device or its applications.

The distinction between consumer and industrial applications should not in any way be construed to minimize or downplay the importance of security to the Internet of Things generally or industrial applications in particular. Indeed, a failure to incorporate adequate security into such applications and systems would mean that cyber-threats will have a greater impact on the physical world than they do today. For example, the injection of fake commands into industrial control systems or smart home systems can result in consequences ranging from mild annoyance—a home being too hot—to injury or death—a car running off the road. This distinction simply seeks to acknowledge federal agencies' experience in regulating consumer safety issues and their importance in endorsing a framework that encourages their responsible use.

The Secure ID Coalition supports the development of a national Internet of Things strategy that recognizes the important distinction between consumer and industrial IoT applications as well as the indispensible role of security in providing the trust necessary for continued adoption of IoT technologies. Countries such as Germany and India have published IoT roadmaps with a heavy emphasis on manufacturing. Industrial IoT applications are essential to increasing U.S. economic competiveness and ensuring the continued global dominance of the country's technology sector. As the U.S. moves toward a national IoT strategy, consideration should be given to the role of consumer identity in building the long-term confidence needed for sustained growth. The federal government should also seek to actively engage with international partners across the public, private, and nonprofit sectors to identify best practices and innovative solutions to some of the most difficult challenges standing in the way of IoT development.

It is in the spirit of ensuring adequate public-private coordination that the Secure ID Coalition also supports the ***Developing Innovation and Growing the Internet of Things (DIGIT) Act*** (S. 2607 / H.R. 5117). This bipartisan bill currently under consideration in Congress would direct the Department of Commerce to convene a working group of federal stakeholders to provide recommendations and a report to Congress regarding the Internet of Things, and would establish a steering committee to be composed of stakeholders outside the federal government to advise the working group.

There is little doubt that the Internet of Things has the potential to dramatically impact our daily lives for the better. What is less certain is the exact form IoT innovations will take and the extent to which an individual innovation will impact our lives. Given these facts, it would be prudent for policymakers to exercise regulatory caution as we gather more information about the specific technologies that will impact our lives and their implications for privacy and security policy. The federal government should continue to actively engage with industry in order to identify the greatest causes of concern and optimism.

Respectfully Submitted,

Kelli A. Emerick
Executive Director