March 13, 2017

Office of Policy Analysis and Development
National Telecommunications & Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W., Room 4725
Washington, D.C. 20230

Re: NTIA Request for Public Comments (RIN 0660 – XC033) – The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

To Whom It May Concern:

The Security Industry Association (SIA) submits the following comments to the National Telecommunications & Information Administration (NTIA) in response to the above-referenced request for public comment (RPC) published in the *Federal Register* on January 13, 2017.

About the Security Industry Association

SIA is a non-profit international trade association representing more than 700 manufacturers and integrators of security and life safety technology, 80 percent of which are small businesses. These technology solutions include, but are not limited to, intrusion detection, video surveillance, fire alarm, fire suppression, access control, mass notification and emergency communications.

Executive Summary

After publishing a green paper entitled *Fostering the Advancement of the Internet of Things* in January 2017*,* NTIA is seeking additional input from stakeholders who submitted comments during an initial request for comment in 2016. The initial comments, in conjunction with numerous public-private forums, provided input to NTIA during the drafting and publication of the 2017 green paper – the primary objective of which is to help define what role the U.S. government should play in promoting IoT growth, investment, and prosperity.

IoT technology is transforming the security industry. The increasing connectivity of security devices multiplies the ability of security practitioners to prevent or quickly address emergencies and to better protect people, property and information. We believe the private sector is in the best position to develop solutions for cybersecurity, data privacy, data management, and standards development. However, the federal government has a critical role to play in infrastructure investment, fostering collaboration with and within the private sector regarding IoT development activities, ensuring full use of available spectrum for device communication, and fostering growth in the skilled workforce the expansion of IoT requires.

NTIA policymakers requested that the 2017 RPC answer the following questions in response to the published green paper:

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

Below are SIA's responses to those four questions from the security industry's perspective:

Question 1: Is our discussion of IoT presented in the green paper regarding the challenges, benefits, and potential role of government accurate and/or complete? Are there issues that we missed, or that we need to reconsider?

NTIA presented thorough recommendations on how private sector stakeholders can voluntarily make efforts to alleviate certain privacy and cybersecurity concerns – i.e. privacy by design, security by design, and voluntarily abiding by the NIST *Framework for Improving Critical Infrastructure Cybersecurity.* The green paper correctly cites that security failures are more likely to occur when security is not a consideration throughout the concept and design process of a product. Privacy and security by design must occur at the outset of engineering IoT products.

In addition, we believe the paper thoroughly and accurately outlines the myriad of benefits IoT growth presents for consumers, the Federal government, and multiple business sectors seeking to maximize labor productivity. Data generated by IoT sensors will exponentially improve the livelihoods of citizens through applications such as wearable technologies, expedited notifications on mobile applications, real-time monitoring of personal health and security, and improved public safety responses – notably FirstNet that was mentioned in the *Enabling IoT Functionality for First Responders* section that improves situational awareness in emergencies. NTIA also acknowledged the need for a robust networked infrastructure that can withstand the increasing levels of data flow. Subsequently, NTIA should continue to champion and encourage "smart city" initiatives to ensure that major metropolitan cities incorporate necessary infrastructure investments into the city planning stages that fully anticipates IoT deployment.

However, there is a significant challenge not explicitly cited in the green paper – an uncertain or hostile legal environment that could deter IoT developers and limit the benefits of IoT devices for consumers. Particularly as developers continue to find ways to make IoT devices more cyber-secure and communicate about installation and operating practices with consumers, they face increased vulnerability to legal exploitation and regulatory overreach based on hypothetical harms. For example, last year IoT developers witnessed actions taken by the Federal Trade Commission (FTC) to dispute a manufacturer's IoT security claims due to alleged vulnerabilities – even though no actual data breach occurred. In another example, a class action suit was filed against a manufacturer insisting that certain high security features used only for sensitive government facilities should be incorporated in typical residential intrusion detection systems, if protection against unwanted entry and property loss is claimed. IoT regulation by litigation is not a transparent or economically desirable policy solution to address concerns, and could be a serious impediment to growth and raise high-cost barriers to entry for small businesses.

Question 2: Is the approach for Departmental action to advance the Internet of Things comprehensive in the areas of engagement? Where does the approach need improvement?

The four areas of engagement outlined on page four of the green paper sufficiently addresses the correct approach needed to foster IoT growth since it incorporates subset issues such as cybersecurity, privacy, and innovation. Concurrently, NTIA created five working groups that will produce multi-stakeholder solutions with equitable consideration. Approach areas could be added to address other issues impacting the IoT ecosystem such as liability protections and small business implications.

Question 3: Are there specific tasks that the Department should engage in that are not covered by the approach?

Once the five working groups convene, a top priority of NTIA should include working with international governments on cross-border data flows. This task could be accomplished through the interagency process. Due to the globalized economy and increased levels of international investment, NTIA, in concert with the U.S. State Department and Trade Representative, should encourage foreign countries with published IoT national strategies to rescind import license requirements and data localization policies that ultimately deter U.S. IoT investment.

If misguided data localization and import requirements are emulated across the globe, it could preclude certain security industry companies from investing in those respective markets due to the growing adoption and efficacy of cloud-based solutions. Such products often utilize the robust data center infrastructure in the United States. When countries mandate that any data collected within a country must be stored in that same country, it is particularly burdensome for small to mid-sized companies seeking growth.

Question 4: What should the next steps be for the Department in fostering the advancement of IoT?

NTIA should continue its leadership role in fostering the advancement of IoT growth by partnering with the private sector. NTIA should also place emphasis on engaging state and local governments in support of the goals and objectives put forth in the NTIA's green paper. A number of state and local governments have asserted a role in governing IoT through legislative means. For example, lawmakers from the Massachusetts Senate have proposed a bill that directs the MA Department of Consumer Affairs to regulate manufacturers of IoT devices that collect "IoT personal data." Any balkanization of rules governing IoT down to the state and local level has the serious potential to limit consumer benefit from IoT and related economic growth, and would not be consistent with the goals outlined by NTIA.

Conclusion

The security industry is optimistic about IoT growth potential and its benefits for the private and public sectors. We strongly support the federal government's efforts to consult with the business community over the future of IoT. SIA also acknowledges and supports NTIA's assertion that introducing, promoting, and implementing standards in the IoT ecosystem should be industry-led. Our members stand ready to offer further input on how policymakers can offer the best guidance on fostering IoT growth in the United States. Both consumer and enterprise IoT offer an enormous opportunity to improve security and life safety products. The Federal government can play a helpful role in promoting IoT investment and preventing barriers that would limit growth. We thank NTIA for convening the public/private sector working groups focused IoT related issues. SIA and its members look forward to participating in future forums.

Sincerely,

Don Erickson

Don Erickson
CEO
Security Industry Association