June 3, 2016

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 0600 – XC024) – 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 published in the *Federal Register* on April 6, 2016.

About the Security Industry Association

SIA is a non-profit international trade association representing approximately 700 global security and life safety solutions providers, nearly 80 percent of whom are classified as small businesses. Our membership is comprised of security manufacturers, integrators, and service providers. SIA member products play a key role in securing numerous components of critical infrastructure such as military installations, federal buildings, airports and seaports, and public transit systems. These technology solutions include, but are not limited to, access control, identity management, biometrics, intrusion detection, video surveillance, fire alarm, fire suppression, gas detection, mass notification and emergency communications.

Executive Summary

In its request for comments, NTIA is seeking input from industry and other stakeholders on both the potential benefits and challenges of "internet of things" (IoT) technologies and what role, if any, the U.S. Government should play in this domain. NTIA also seeks to identify ways the U.S. government can partner with the private sector to foster advancement of IoT technologies.

IoT 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 standards development activities, ensuring full use of available spectrum for device communication and fostering growth in the skilled workforce the expansion of IoT requires.

By 2025, rapid growth of the IoT is expected to contribute up to $11 trillion per year to the global economy. The continued leadership of the United States on issues surrounding IoT development and deployment is essential to ensuring policies that allow for innovation and growth and maximize the benefits of IoT to society.

Benefits of IoT Technology for Security Applications

IoT allows systems and devices to perform better, smarter and in a more coordinated fashion, especially within the physical security domain where the promise of creating a security climate that is more preventive than reactive. IoT networked sensors are already improving the effectiveness of security solutions in the consumer, commercial and government arenas by providing real-time connectivity and data collection.

A notable current example has been the transition from analog surveillance cameras to internet protocol (IP) cameras. As of 2008, consumers converted nearly 50 percent of video surveillance systems from analog to IP cameras,[1] a figure that is much higher now. IP cameras offer dramatically improved video quality, allow on-board data storage and video analytics, improve scalability, and lower installation and maintenance costs. IP cameras have become the global standard for video surveillance in just a few years due to these enhanced, network enabled capabilities.

Another example of an IoT security application would be a classroom equipped with network-based audio/visual recording platforms utilizing IP cameras and a connected microphone. While such systems are used primarily for educational purposes, controlled by the instructor, the same audio sensor can detect and respond to certain sounds such as gunshots, broken glass and verbal aggression that indicates an emergency situation. IP cameras can broadcast video and other data to law enforcement and other first responders in real-time, serving as a security solution during an emergency.[2]

Potential Challenges

While the full scope of future use of IoT and the data it generates is unclear, emerging issues related to cybersecurity, data privacy, data management, interoperability and spectrum needs present challenges that should be addressed. However, we believe the private sector is in the best position to develop solutions to these challenges, and that a non-regulatory approach to policy will help ensure maturation of IoT technologies.

SIA members utilize a wide variety of standards development bodies and organizations for guidance, best practice resources, and educational services that enable companies to manufacture, integrate and maintain high quality, cyber-secure products. SIA is addressing emerging cyber issues in part through recent formation of the SIA Cyber Security Advisory Board, consisting of subject matter experts will provide guidance to the industry. The first publication, “The Beginners Guide to Product and System Hardening” relating to IoT devices, outlines basic safeguards to help protect security products, systems and services against failure from cyberattack.[3] NIST has also issued two sets of voluntary guidance

concerning data encryption – *Advanced Encryption Standard Algorithm*[4] and *Guidance to Storage Encryption Technology for End-User Devices*[5] – that are widely-utilized by SIA member manufacturers and integrators.

SIA members also develop technology solutions that incorporate "privacy by design," protecting personally identifiable information from design to manufacture to implementation and deployment. SIA released the *Security Industry Association Privacy Framework*[6] to outline a core set of principles and best practices the industry is working to implement in the deployment of electronic security technologies protecting people, data, sensitive information, and assets.

In this regard, we are concerned about the U.S. Federal Trade Commission's proposal[7] on data minimization. While well intended to support the concept that companies should limit the data they collect, retain, and dispose of once no longer needed, this proposal could preclude de-identification protocols (storing and sharing the data without revealing the identity of the individuals involved) which ultimately protect sensitive data without compromising its integrity[8].

The issue of interoperability standards, or lack thereof, is another potential challenge identified by IoT experts within SIA. According to the AllSeen Alliance, a cross-industry consortium dedicated to enabling the interoperability of billions of devices, services and applications that comprise the IoT, the goal of IoT standards should be[9]:

> *To create interoperable products that can discover, connect, and interact directly with other nearby devices, systems, and services regardless of transport layer, device type, platform, operating system, or brand.*

Current standards will require certain adjustments that incorporate the migration of legacy products to network IP. For example, SIA, as an ANSI-accredited standards development organization, has developed a protocol to foster interoperability among security devices, titled the SIA Open Supervised Device Protocol (OSDP[10]). This communications protocol allows peripheral devices, such as card readers and biometric readers, to easily and securely interface with control panels or other security management systems. In its current version, OSDP reduces physical barriers to achieving interoperability such as shipping prototypes to numerous vendors for testing. The underlying source code is another aspect of the tool that can be leveraged by device manufacturers in developing their OSDP interoperable products.

Finally, IoT experts within SIA continue to convey concerns over potential sensor data overload, and the impact it could have on consumers, enterprises, and the public sector. Without proper human oversight in managing and analyzing the massive flow of data collected by IoT devices, these products may not meet performance expectations. However, addressing this need is complicated by the fact that by 2018, the United States could experience a skilled workforce shortage of nearly 200,000 workers educated in data science, according to recent reports. [11]

How the Federal Government Can to Partner with the Private Sector to Advance IoT

The federal government should focus on fostering collaboration between the public and private sectors in eliminating barriers to deployment, ensuring adequate spectrum to support IoT, and development of voluntary standards. It should also work to resolve jurisdictional overlap between agencies that could impede this growth. Not only should the development of standards within the private sector be

encouraged, NTIA should also work to ensure that National Institute of Standards and Technology (NIST) continues to play an instrumental role in developing voluntary standards consistent with the National Technology Transfer and Advancement Act of 1995.

Legislation could also play a helpful role in promoting successful IoT growth, so long as it is not prescriptive. For example, S. 2607; H.R. 5117, the Developing Innovation and Growing Internet of Things (DIGIT) Act,[12] would require the public sector to consult with private industry on IoT deployment procedures, policies or programs related to consumer privacy (and security), and spectrum availability.

There could also be a significant role or the federal government, through its K12 and higher education programs, to encourage practices that ensure the future workforce obtains basic data science management/analytic skills prior to entering the workforce. Furthermore, it should have the goal of working in partnership with the private sector to ensure that an adequate number of individuals with high-level skillsets needed to work with IoT systems are trained.

The federal government should also work to prevent a lack of infrastructure planning and investment that could put the U.S. economy at a competitive disadvantage compared to nations that have begun constructing smart cities, grids, and transportation systems. The case of India offers an example of both investment and policies that could inhibit IoT. Investment experts have proclaimed India as the next emerging market in IoT due to the Indian national strategy that established a policy framework to cultivate IoT. India's strategy also showcased the government's plan to develop 100 smart cities[13] – financed by a $7.4 billion investment, plus a state and municipal matching grant program until 2020.

While this initiative may appear promising and remunerative for foreign investment, the Indian government will mandate import license requirements for certain connected devices. In return, this provision enumerates the Indian government to charge foreign device manufacturers high fees in order to access the Indian market, or block them altogether.[14] This anti-competitive policy is compounded by localized cross-border data flow restrictions. Currently, India requires servers that support IoT to be located in the country if it services Indian customers. In this case the ambitious IoT investment by the Indian government is put at significant risk of failure by myopic regulations and data localization requirements.

The United States took a step to spur IoT related infrastructure investment in September 2015 when the U.S. Department of Transportation (USDOT) launched a *Smart City Challenge.* USDOT[15] has pledged up to $40 million to one city to help it define what it means to be a "Smart City "and become the country's first city to fully integrate innovative technologies – self-driving cars, connected vehicles, public safety enhancements and smart sensors – into their transportation network. SIA commends the administration's leadership on the smart city initiative, and hope the $40 million investment will further position the United States to architect a sustainable, robust, and technologically-advanced cities.

Conclusion

SIA is enthusiastic about the IoT growth potential for both the private and public sectors, and we strongly support the U.S. Federal government's efforts to consult with the business community over the future of IoT. 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 enhance security and life safety applications. The Federal government can play a helpful role in promoting IoT investment while refraining from policies that would limit growth.

We understand NTIA intends to convene a public/private sector working group focused IoT related issues. SIA and its members look forward to participating.

Sincerely,

Don Erickson
CEO
Security Industry Association

---

[1] Rob Morello, Product Sales Manager – Pelco, *available at*¸ http://www.cablinginstall.com/articles/print/volume-13/issue-6/contents/security/added-features-amp-persistence-increase-ip-camerasrsquo-market-share.html

[2] David Antar, President and CEO, IPVideo Corp. *SIA Webcastr - The Takeover: How the Industrial Internet of Things (IoT) Impacts the Security Industry,* (May 20, 2016), *available at,* http://www.siaonline.org/Pages/Webcasts/SIA-Emerging-Technologies-Webcast-Series2.aspx

[3] Beginners Guide to Product and System Hardening (March 2016), https://www.securityindustry.org/SiteAssets/Technology/SIA%20Cybersecurity%20Advisory%20Board%20-%20Beginners%20Guide.pdf

[4] NIST Advanced Encryption Standard Algorithm, (November 26, 2001), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[5] NIST Guidance to Storage Encryption Technology for End-User Devices, (November 2007), http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

[6] Security Industry Association Privacy Framework, (September 2014), https://www.securityindustry.org/SiteAssets/GovernmentRelations/gr-privacy-framework.pdf

[7] Internet of Things: Privacy & Security in a Connected World, *FTC Staff Report,* (January 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[8] Ann Cavoukian and Daniel Castro, *Setting the Record Straight: De-Identification Does Work,* (June 16, 2014), *available at*, https://itif.org/publications/2014/06/16/setting-record-straight-de-identification-does-work

[9] The AllSeen Alliance's framework drafted by AllJoyn, *available at,* https://allseenalliance.org/alliance/faq

[10] The Security Industry Association's Open Supervised Device Protocol, *available at,* http://sia-sharepoint/Document%20Library/A%20Smart%20Protocol%20for%20Smart%20Devices-FINAL.pdf

[11] Adam Popescu, *How Universities are Adapting to the Internet of Things Revolutions,* (April 14, 2014), *available at* http://www.forbes.com/sites/ptc/2014/04/14/how-is-academia-adapting-to-the-internet-of-things-revolution/#33b85dc35b9f

[12] Security Industry Association Letter of Support: S. 2607, (April 26, 2016), http://securityadvocates.org/sia/SIA-Letter-of-Support-S-2607.pdf

[13] Government of India, Ministry of Communication & Information Technology – Department of Telecommunications, *National Telecom M2M Roadmap,* (May 2015), *available at* http://www.dot.gov.in/sites/default/files/Draft%20National%20Telecom%20M2M%20Roadmap.pdf

[14] Joshua New & Daniel Castro, Center for Data Innovation, *Why Countries Need National Strategies for the Internet of Thing,* (December 16, 2015), https://www.datainnovation.org/2015/06/what-india-gets-right-and-wrong-about-the-internet-of-things/

[15] U.S. Department of Transportation Smart City Challenge, (2016), https://www.transportation.gov/smartcity