Coalition for Cybersecurity Policy and Law

Coalition for Cybersecurity Policy and Law
575 Seventh Street, NW, Washington, DC 20004

June 2, 2016

VIA EMAIL: iotrfc2016@ntia.doc.gov

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Attn: IOT RFC 2016
Washington, DC 20230

Re: Comments of the Coalition for Cybersecurity Policy & Law

The Coalition for Cybersecurity Policy & Law ("Coalition") submits the following comments in response to the Request for Comment ("RFC") that the National Telecommunications and Information Administration ("NTIA") issued on April 6, 2016 regarding the benefits of and challenges to the IoT market and the appropriate role of the federal government with respect to this market. The coalition appreciates the opportunity to provide these comments and participate in this important discussion. As the IoT market continues to experience tremendous growth, it is critically important to consumer privacy, consumer and public safety, and the continued development of the IoT market that connected devices be secure.

The Coalition is comprised of leading companies with a specialty in cybersecurity products and services dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies.[1] We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity, and we are supportive of the development of a flexible set of security controls that will encourage the adoption of stronger security measures in the IoT market while still permitting companies to develop new and innovative security products and services.

The Coalition believes that the IoT market holds great promise for both consumers and businesses; however, this promise will be fully realized only if IoT products and services are secure. A failure to incorporate appropriate security into these products and services could result in substantial harm to consumers in the event their personal information is stolen, or they lose control of critical device functionality. Strong security is also important to the development of consumer trust in these products and services. The government can help foster consumer trust in the IoT marketplace by encouraging manufacturers to be transparent about the level of security that they have incorporated into their devices. Providing consumers with better information

[1] The views expressed in these comments reflect the consensus views of the Coalition, and do not necessarily reflect the views of any individual Coalition member. For more information on the Coalition, see www.cybersecuritycoalition.org.

about the security of the devices they use and rely on empowers consumer to choose the device that fits their desired level of security, which, in turn, allows the market to determine the appropriate level of security. The Coalition supports efforts by the federal government to encourage companies to incorporate security into their products from the design stage all the way through delivery to consumers or businesses. The Coalition also believes that the federal government should emphasize the importance of supply chain risk management and software updating in the IoT market. The Coalition recognizes that not all products and services in the IoT market will require the same level of protection, as the market spans a number of industries and involves both business-to-business transactions and business-to-consumer sales. Therefore, the Coalition supports a flexible rather than prescriptive approach in setting security controls in this space.

I. Consumers Benefit from the Development of the IoT

The IoT market has the potential to provide consumers and businesses with tremendous benefits by improving the efficiency, convenience, and safety with which individuals perform a wide variety of tasks. The Federal Trade Commission ("FTC") identified some of the benefits to consumers developing out of the IoT market in its report "Internet of Things: Privacy & Security in a Connected World."[2] Specifically, the report noted that the use of IoT devices in the medical context has provided individuals who are unable to visit a doctor with improved treatment options and has provided doctors with better information about their patients' health.[3] The report also stated that the incorporation of IoT devices into cars can improve driver safety by notifying drivers of dangerous road conditions, providing drivers with real-time vehicle diagnostics, and automatically alerting first responders when the vehicle is involved in a crash.[4]

The development of the IoT market also benefits the broader economy. At least one study estimated that the annual value of the IoT market could be between $4 trillion and just over $11 trillion by 2025.[5] This level of production would create countless jobs for individuals and would strengthen the economy as a whole. Consumers and businesses will also benefit from an explosion of new products and services that will make performing a variety of tasks easier and more efficient.

Although the IoT market already provides significant benefits to consumers and businesses, it is also subject to several security risks that could threaten the development of the market. The FTC identified three such risks in its report: (1) the risk of unauthorized access to

[2] Federal Trade Commission, *Internet of Things: Privacy & Security in a Connected World* 7 (January 2015), available at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
[3] *Id.*
[4] *Id.* at 9.
[5] McKinsey Global Institute, *The Internet of Things: Mapping The Value Beyond The Hype* 7 (June 2015), available at http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

IoT systems, and misuse of personal information contained within those systems; (2) the use of IoT systems as a launching pad to facilitate attacks on other systems; and (3) safety risks arising out of security breaches that interfere with the proper operation of IoT systems.[6] Failing to address these risks could threaten the development of the IoT market by eroding consumer trust. Therefore, the Coalition supports the development of flexible, targeted security controls that will mitigate these risks. These controls could include the implementation of embedded security and roots of trust where feasible.

II. The US Department of Commerce Should Facilitate the Development of Flexible Security Controls

The US Department of Commerce (Commerce) can play an important role in improving the level of security across the IoT market by facilitating a discussion about the types of security controls that companies should implement and the related standards that can ensure interoperability and quality of these controls. Raising awareness among the key actors in the IoT market about the security threats they face and the steps they can take to protect their products and services will help improve security across this space.

The Coalition supports the continued reliance on voluntary consensus-based, industry-led standards setting processes to set cybersecurity standards for the IoT market. Such an approach would be consistent with the requirements of the National Technology Transfer and Advancement Act and OMB Circular A-119. This approach was also highly successful when used by the National Institute of Standards and Technology to develop the Cybersecurity Framework. Further, reliance on a voluntary, consensus-based, industry-led approach to setting cybersecurity standards in the IoT market is appropriate dues to the diverse nature of the IoT market. The IoT market crosses multiple industries and covers a wide array of devices with varying functionalities and capabilities, and varying degrees of security risk. Not all IoT devices could be used to cause harm to individuals if an unauthorized person gains access to the device; however, some devices like medical devices and connected cars, present substantial safety risks if control of the device is not properly restricted. Additionally, the businesses that are involved in the IoT market vary significantly with respect to their size, resources, and the sophistication of their products. A voluntary, consensus-based, industry-led approach to setting cybersecurity standards for the IoT market would be able to account for this level of diversity in the market, while a prescriptive government-led approach is far more likely to set standards that may be overly burdensome and may restrict innovation in the market.

A flexible approach is also consistent with the steps that the FTC has taken with respect to the security of consumer information. The FTC's "reasonable security" standard enables businesses to tailor their security procedures and protections to their specific needs. This flexibility increases the likelihood of adoption amongst businesses and consumers, which is vital to the effectiveness of such security products and services. A flexible approach also encourages

[6] *Internet of Things: Privacy & Security in a Connected World* 10 (January 2015)

Coalition for Cybersecurity Policy and Law
575 Seventh Street, NW, Washington, DC 20004

innovation that could result in new security products and services that will allow participants in the IoT market to attain better security results. The Commission believes that greater transparency regarding the security of the devices in the IoT marketplace is essential to attain these benefits, as providing consumers with more information about security will enable them to make informed decisions regarding the appropriate level of security for their needs.

III. Issue Areas that Should Be Addressed By the Security Controls

The Coalition encourages Commerce to include the following topics in its discussions about the appropriate security controls in the IoT market: (1) vulnerability disclosure, (2) supply chain risk management and (3) updating and patching software. These areas are of particular importance for the security of the IoT market. IoT developers and users can take a number of steps in these areas, particularly with respect to patch management, to enhance security. However, it is important for Commerce to provide greater clarity in these areas to help companies understand the steps they should take to strengthen their security controls and to promote the use of security standards in IoT.

Vulnerability Disclosure. Notifying market participants about identified vulnerabilities is particularly important in the IoT market because (1) the proliferation of IoT devices has increased the number of opportunities that an attacker has to gain access to personal and sensitive information; (2) vulnerabilities in IoT devices could facilitate attacks on consumers' networks or on other systems by enabling attackers to create larger botnets, and (3) vulnerabilities in some IoT devices could threaten consumers' physical safety as well as the safety of the broader public.[7] The possibility of consumer harm arising from un-remedied vulnerabilities in IoT devices poses a substantial threat to consumer trust in the IoT market, which is essential to its continued development and expansion. The Coalition believes that the adoption of vulnerability disclosure policies by market participants is an important step in protecting consumers and securing their trust in the IoT market. Therefore, the Coalition recommends that the Department of Commerce actively encourage companies with IoT products to adopt vulnerability disclosure policies. The Coalition also believes that the Department of Commerce can play an important role in promoting the establishment of generally accepted standards pertaining to the disclosure of vulnerabilities. The Coalition recognizes that NTIA has already begun this work, and it supports NTIA's efforts in this area. However, the Coalition believes that more should be done to encourage participants in the IoT market to adopt policies that promote the disclosure of vulnerabilities to other market participants.

Supply Chain Risk Management. It is important for all companies to understand the security of the supply chain through which they acquire their IT infrastructure; however, it is particularly important in the IoT market where companies are integrating internet connectivity into their products. The NIST Framework Core incorporates consideration of an entity's position

[7] *See* Federal Trade Commission, *Internet of Things: Privacy & Security in a Connected World*, 10 – 12 (January 2015).

in the overall supply chain when identifying cyber assets to be protected, but it does not address the security of a company's supply chain. Supply chain vulnerabilities present security risks to both businesses and consumers in the IoT market, yet greater clarity is needed about the measures that companies should take to ensure that malicious code or other vulnerabilities are not introduced into their products as they are being developed and manufactured. The Coalition encourages NTIA to look to prior work done by NIST with respect to supply chain management as a starting point for further discussion. Specifically, following the release of the NIST Cybersecurity Framework, NIST issued SP 800-161, a guidance document pertaining to securing an organization's supply chain.[8] In October 2015, NIST also held a workshop on Best Practices in Cyber Supply Chain Risk Management. This work addresses areas such as vendor selection and controls, detection and prevention of vulnerabilities in hardware and software, and implementation of controls on software design, loading, and testing processes. The Coalition also believes that an important element of supply chain risk management is embedding security into devices and establishing secure hardware roots of trust. The Coalition encourages NTIA to foster discussion among participants in the IoT market about how vulnerabilities in their supply chain can harm efforts to add these security measures to their products.

Updating and Patching. Identifying and patching security vulnerabilities is critically important to maintaining the security of software products. Therefore, it is essential that the manufacturers of IoT products continue to provide support to such products. To encourage such support within the IoT market, Commerce should initiate a discussion about the challenges involved in updating IoT devices and how these challenges can be overcome. In its report on the IoT market, the FTC identified some of the challenges that the market faces in promoting the patching of identified vulnerabilities: (1) IoT devices that are designed to be inexpensive and disposable are more difficult to update; (2) consumers are often unaware of available security patches; and (3) companies may lack economic incentives to provide ongoing support and security updates. The Coalition also encourages Commerce to facilitate the development of industry standards with respect to implementing an effective patch management program. The Coalition believes that Commerce can play an important role in the development of specific guidelines that participants in the IoT market should follow when implementing patches to identified vulnerabilities to the security of their devices and systems. Having clear patch management guidelines is particularly important in the IoT market as a significant number of participants in this market may be new to the technology industry and may not know how to implement an effective patch management program or understand the importance of such a program. These guidelines should encourage participants in the IoT market to collaborate with third parties, to plan by design for evidence capture, and to segment and isolate unpatched systems until the entity is confident that the system is "clear." The Coalition believes that Commerce is well positioned to facilitate the development of such guidelines and to promote their adoption across the IoT market.

[8] NIST, SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations (April 2015), available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

Coalition for Cybersecurity Policy and Law
575 Seventh Street, NW, Washington, DC 20004

IV. Conclusion

The Coalition thanks the NTIA for the opportunity to comment in this important effort. We look forward to working with you as this process moves forward and to participating in any further discussions pertaining to the security of the IoT market.

Sincerely,

Ari Schwartz
Coordinator