



1200 G Street, NW  
Suite 500  
Washington, DC 20005

P: +1 202-628-6380  
W: [www.atis.org](http://www.atis.org)

July 28, 2017

Evelyn L. Remaley  
Deputy Associate Administrator  
National Telecommunications and Information Administration  
U.S. Department of Commerce  
1401 Constitution Avenue, NW  
Room 472  
Washington, D.C. 20230

Re: Input to Promoting Stakeholder Action against Botnets and Other Automated Threats  
Docket No. 170602536-7536-01

Dear Ms. Remaley:

The Alliance for Telecommunications Industry Solutions (ATIS) is pleased to provide its input to the *Request for Comments (RFC)* released June 8, 2017, by the National Telecommunications and Information Administration (NTIA). In the *RFC*, NTIA requests input on actions that can be taken to address automated and distributed threats to the digital ecosystem as part of the activity directed by the President in Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." ATIS submits these comments to provide information regarding industry efforts to foster security associated with the Internet of Things (IoT) and to identify and mitigate cybersecurity-related risks.

#### About ATIS

ATIS is a technology and solutions development organization for the information and communications technologies (ICT) sector that advances pressing business priorities, including cybersecurity, next generation wireless and wireline network technologies (LTE, 5G, NFV), emergency services, quality of service, billing support, and operations. ATIS' membership includes stakeholders from wireline and wireless service providers, equipment manufacturers, software developers, consumer electronics companies, digital rights management companies, and internet service providers.<sup>1</sup> ATIS represents the ICT sector both in the U.S. and globally through its roles as the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, and member of the Inter-American Telecommunication Commission (CITEL), and as a member and contributor to the International Telecommunication Union (ITU).

---

<sup>1</sup> A list of ATIS' members can be found on the ATIS website at: [http://www.atis.org/01\\_membership/members/](http://www.atis.org/01_membership/members/).

ATIS works to foster network security and reliability, and several ATIS forums are tasked with addressing cybersecurity issues, including ATIS' Cybersecurity Ad Hoc. This ad hoc was launched in July 2015 to undertake a multi-step analysis of cybersecurity issues. The group is developing an overall industry cybersecurity framework focused on the needs of the ICT industry, as well as developing practices in relation to the transition towards NFV/Cloud based infrastructure and the protection of security in the context of complex supply chains.

### **Endpoint Prevention -- IoT Security**

In the *RFC*, NTIA note the importance of securing endpoints, particularly IoT devices.<sup>2</sup> ATIS notes that there are significant efforts underway within the industry to examine on IoT security, including work recently completed by ATIS' Cybersecurity Ad Hoc.

In May 2017, the ATIS Cybersecurity Ad Hoc has published its Securing Internet of Things (IoT) Services Involving Network Operators (ATIS-I-0000056).<sup>3</sup> This report examines several different scenarios that characterize different relationships and levels of partnering that may exist between a network operator and an IoT service provider, noting that shared responsibility for securing the service may exist. The report also recommends practices that may improve the security of IoT systems. For example, the report recommends that IoT services using a standard IoT platform should still be subject to a comprehensive security threat analysis leading to a secure solution design and secure operating procedures. Moreover, the report recommends that service designers should understand and use the security features provided by the IoT platform, while also providing layered security using multiple approaches.

The report also includes a description of other industry activities relevant to IoT security, which are listed on the table below.<sup>4</sup>

<b>Working Group</b>	<b>Charter</b>
<b>IPSO Alliance</b> (Sep 2008)	Establish <i>Internet Protocol (IP)</i> as the network to interconnect smart objects and allow existing infrastructure to be readily used without translation gateways or proxies.
<b>IoT-A</b> (2010-2013)	Developed an architectural <i>reference model</i> to allow seamless integration of heterogeneous IoT technologies into a coherent architecture to realize 'Internet of Things' rather than 'Intranet of Things'.

<sup>2</sup> 82 *Federal Register* 27042, 27043.

<sup>3</sup> This document is available at no charge from the ATIS White Paper repository at [http://www.atis.org/01\\_resources/whitepapers.asp](http://www.atis.org/01_resources/whitepapers.asp).

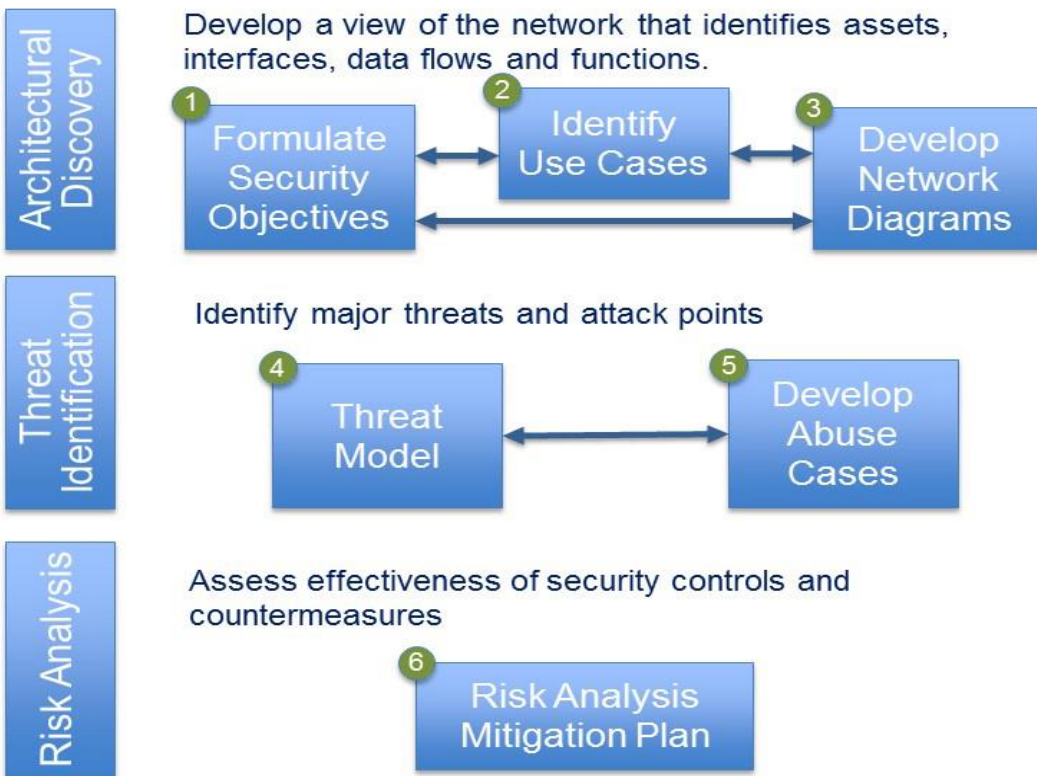
<sup>4</sup> Securing Internet of Things (IoT) Services Involving Network Operators (ATIS-I-0000056), Table 4.1.

Working Group	Charter
<b>AllSeen Alliance</b> (2013)	Collaborate for an open, universal IoT software framework across devices and industry applications, based on AllJoyn <i>open source project</i> , originally developed by Qualcomm but now released to community developers.
<b>Industrial Internet Consortium</b> (Mar 2014)	Accelerate development and adoption of <i>intelligent industrial automation</i> for public use cases.
<b>HyperCat</b> (May 2014)	Develop an open specification for IoT that will make data available in a way that others could make use of it, through a <i>thin interoperability layer</i> .
<b>Open Interconnect Consortium</b> (Jul 2014)	Define interoperable <i>device communication standards</i> (for peer-to-peer, mesh & bridging, reporting & control etc.) across verticals, and provide an <i>open source</i> implementation
<b>IEEE P2413</b> (Jul 2014)	Create a <i>standard interoperability architecture</i> and define commonly understood data objects, for information sharing across IoT systems.
<b>OMA LWM2M (2014)</b>	Proposed a new <i>Light-weight M2M protocol standard</i> , based on client-server model for remote management of M2M devices and related service enablement
<b>oneM2M (July 2012)</b>	There is a need for a common, efficient, easily and widely available M2M Service Layer, which can be readily embedded within various hardware and software.
<b>Cloud Security Alliance IoT Security Guidance for Early Adopters of the Internet of Things (IoT)</b>	The Cloud Security Alliance IoT Working Group focuses on understanding the relevant use cases for IoT deployments and defining actionable guidance for security practitioners to secure their implementations
<b>NIST SP 800-183</b>	A composability model and vocabulary that defines principles common to most, if not all networks of things, is needed to address the question: “What is the science, if any, underlying IoT?”
<b>GSM Association “Internet of Things (IoT) Security Guidelines”</b>	To provide high-level discussion of challenges, IoT models, risk assessments, and solution spaces. To give the implementer of an IoT technology or service a set of design guidelines for building a secure product.

### **Attack Mitigation –Architectural Risk Analysis**

The *RFC* also seeks comment on minimizing the impact of botnet behavior by identifying and disrupting malicious behaviors.<sup>5</sup> To facilitate the identification of risks, ATIS has developed a process for performing an Architectural Risk Analysis (ARA) on ICT solutions to enable the proactive development of cybersecurity risk management steps for these solutions.

This process, defined in the Cybersecurity Architectural Risk Analysis Process (ATIS-I-0000057), includes procedures to determine security goals, identify and assess potential risks, and develop proactive steps to mitigate identified risks.<sup>6</sup>



This document also includes an illustrative example of the use of the process for a hypothetical health monitoring device and associated services that are delivered in an ICT service provider-managed context. Finally, some potential areas for additional work are identified to broaden the scope of the ARA Process and to further simplify its application.

<sup>5</sup> 82 *Federal Register* 27042, 27043.

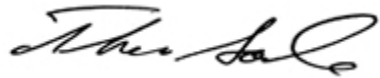
<sup>6</sup> Cybersecurity Architectural Risk Analysis Process at p. 2. This document is available at no charge from the ATIS White Paper repository at [http://www.atis.org/01\\_resources/whitepapers.asp](http://www.atis.org/01_resources/whitepapers.asp).

Letter to E. Remaley  
July 28, 2017  
Page 5

ATIS recommends that the ICT industry perform regular security reviews using processes such as ATIS' ARA to determine security goals, identify and assess potential risks, and develop proactive steps to mitigate identified risks. These analysis processes should leverage existing and appropriate security frameworks and best practices.

If there are any questions regarding this matter or additional information is required, please do not hesitate to contact the undersigned.

Sincerely,

A handwritten signature in black ink, appearing to read "Thomas Goode". The signature is written in a cursive style with a large, stylized initial "T".

Thomas Goode  
ATIS General Counsel