1200 G Street, NW
Suite 500
Washington, DC 20005

P: +1 202-628-6380
W: www.atis.org

April 18, 2018

National Institute of Standards and Technology
Attn: Information Technology Laboratory
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899

Re: Input to NIST Interagency Report (NISTIR) 8200, *Status of International Cybersecurity Standardization for Internet of Things (IoT)*

NIST Information Technology Laboratory:

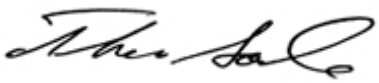
The Alliance for Telecommunications Industry Solutions (ATIS) is pleased to provide input to the draft NIST Interagency Report (NISTIR) 8200, *Status of International Cybersecurity Standardization for Internet of Things (IoT)* that was released February 2018 by the National Institute of Standards and Technology (NIST).

By way of background, ATIS is a technology and solutions development organization for the information and communications technologies (ICT) sector that advances pressing business priorities. ATIS represents the ICT sector 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 contributor to the International Telecommunication Union (ITU). ATIS members include wireline and wireless service providers, equipment manufacturers, software developers, consumer electronics companies, digital rights management companies, and internet service providers.

The attached input, which was developed by the ATIS Cybersecurity Ad Hoc, recommends edits to the NISTIR. ATIS' Cybersecurity Ad Hoc was launched in July 2015 to undertake a multi-step analysis of cybersecurity issues. The group has developed a cybersecurity framework focused on the needs of the ICT industry, evaluated cybersecurity issues associated with the transition towards NFV/Cloud based infrastructure and recommended practices related to the protection of security in the context of complex supply chains.

If you have any questions, please do not hesitate to contact me.

Sincerely,



Tom Goode
ATIS General Counsel

Comment Template for Draft NIST Interagency Report (NISTIR) 8200 -- Status of International Cybersecurity Standardization for the Internet of Things (IoT)

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
1		Editorial	100	Incorrect date.	On April 25, *2017*, the IICS WG established an Internet of Things (IoT) Task Group to determine the current state of international cybersecurity standards development for IoT.
2		Major	131, 140	ATIS recommends the addition of a 6th application area for IoT addressing Wide Area Networked IoT devices. This application area presents unique IoT security requirements and introduces additional standards for consideration (e.g. Low Power Wide Area unlicensed technologies such as provided by the LoRa Alliance - www.lora-alliance.org) and others. This area is also of specific interest to new 3GPP standards such as NarrowBand IoT (NB-IoT) and emerging 5G IoT developments. Additionally, this application area could be scoped to include UAV technologies which are now introducing unique challenges in the IoT space with additional emerging standards.	… ***six*** IoT technology application areas are described … Wide Area Networking in support of metering applications (e.g. utilities), environmental air pollution monitoring, radiation leak monitoring, water quality monitoring, agricultural management, smart cities and UAVs.

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
3		Major	329, 335	The current characterization that IoT consists of two foundational concepts appears to ignore the existence of IoT servers (either physical or cloud-based) that manage the IoT application. Indeed, ATIS generally considers an IoT system to include IoT components that are networked to IoT servers in support of the IoT application. The document may assume that IoT servers are simply IoT components, however, the text gives no indication of this assumption. IoT servers, both physical/dedicated or cloud-based, play a key role in IoT security particularly related to authentication as well as offline management (e.g. software updates) and can provide an additional threat surface for IoT attacks. An excellent example of an IoT architecture showing the role of a service entity has been developed by oneM2M, a global initiative in which ATIS is a partner organization.	The Internet of Things consists of ***three*** foundational concepts: … • IoT Servers which operate in conjunction with a network of IoT components to manage and provide IoT services and applications. NOTE: it may be useful to reference IoT servers in the subsequent description of IoT systems. An example architecture is provided by oneM2M (http://www.onem2m.org/application-developer-guide/architecture or http://www.onem2m.org/application-developer-guide/use-case).

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
4		Major	427, 448	ATIS believes that Secondary Capabilities of an IoT Component should include programmability and configurability.	**Programmability** Whether or not an IoT Component is programmable represents a major cybersecurity consideration. Hard programmed devices are not susceptible to malicious code insertion but cannot be subsequently updated to correct newly discovered security vulnerabilities. Actual programming may require a separate network-accessible maintenance-specific authenticated role or may require local / manual support. **Configurability** Many IoT components will require both default and user-specific configuration. Devices may be configured through a separate network-accessible maintenance-specific authenticated role or may require local / manual support. Configuration data can include access credentials, server names or network specific configuration parameters (e.g. proxy server).

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
5		Major	475	It would be very useful to describe the large variety of threat surfaces associated with the connected vehicle use case. Much of the current text addresses SCMS for V2X communication. However, there are a significant number of additional threat surfaces that should be recognized. As such we suggest an additional paragraph at line 475.	The Connected Vehicle application area presents a particularly large number of threat surfaces due in part to the complexity of a vehicle as an IoT component. Threat surfaces may include: • Internet accessible web-based services provided by the vehicle including both entertainment systems as well as maintenance related functions. • Direct Cellular 3G, 4G and 5G service interfaces for WAN access (for both entertainment and maintenance functions). • Internal vehicle Bluetooth and other Near Field Communications (NFC) systems typically integrated in the vehicle to facilitate entertainment and maintenance operations • Satellite radio interfaces including GPS and XM. • Vehicle integrated Wi-Fi interfaces for both entertainment and maintenance operations. • Internal physically connected interfaces such as USB, CD and SD memory card connections. • Electric vehicle charging station interfaces • Wireless vehicle systems such as Wireless Sensors (e.g., TPMS, RKE). • Internal maintenance ports. • Counterfeit parts (inserted during maintenance operations). • V2x communications.

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
					An example of V2x security capabilities is provided below.
6		Major	761	Given comment 2 listed above, it would seem appropriate to add a small section noting at least one example of Wide Area Network based IoT. A potential example in this case is UAV (although other specific use cases covering meter reading, location services, or critical infrastructure monitoring also could be used).	**Wide Area Network IoT Applications** https://access.atis.org/apps/group_public/download.php/36134/ATIS-I-0000060.pdf https://access.atis.org/apps/group_public/download.php/35648/ATIS-I-0000059.pdf ATIS offers the above-referenced white papers for source material to provide a short example of WAN based IoT.