Dear Interagency International Cybersecurity Standardization Working Group,

Thank you for the opportunity to provide feedback on the draft NIST 8200 Interagency Report on the Status of International Cybersecurity Standardization of the Internet of Things (IoT). ISACA applauds NIST for developing this framework. In the pages that follow, ISACA has provided brief comments for the Group's review and consideration.

As you well know, in this fast-changing environment, IoT cybersecurity will likely evolve and change quickly. ISACA believes the framework NIST has developed is an excellent foundation and helpful first step for the community. As changes occur and updates are required in this area, we look forward to participating with the NIST community to support those efforts.

Also, ISACA recommends, similar to the NIST Cybersecurity Framework, that recommendations and guidance published in this report be voluntary.

Pleases find our comments attached.

Best,

Jennifer Gremmels

ISACA

February 12, 2018

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		Minor	1237	Cybersecurity should be seen as the measures taken to manage the overall risk	as the prevention of -> as the measures taken to prevent
2		Minor	Line. 1263, pg. 32	In general Figure 11 is difficult to follow. Specifically, it is not clear how authorization, authentication and IoT Inter-sector Interactions are threats.	Remove authorization, authentication, and Inter-sector Interactions as New Threat Examples because they are necessary components of an IoT network.
3		Minor	Line 1276, pg. 34	Strengthen the sentence to emphasize the importance of integrity in an IoT network. Availability is critical as stated, but integrity is equally as important when public safety and the enterprise mission are at risk.	Change "sufficient focus" to "emphasis on".
4		Minor	1278	Medical devices also have a strong need for availability (this is mentioned on line 1549)	prioritize integrity -> prioritize integrity and availability
5		Editorial	1320	systems should be plural?	system so that -> systems so that
6	NIST SP 800-30	Major	Line 1340, pg. 36; and chapter overall	The last sentence ending on Line 1340 references NIST SP 800-30 *Guide for Conducting Risk Assessments,* but it doesn't emphasize following the entire risk assessment process. That is, once risks are identified, organizations should identify risk response approaches and monitoring processes. The complete risk assessment process should be followed for each IoT network and the document should emphasize this.	Add additional language in the paragraph ending on Line 1340 that states that organizations should identify appropriate risk responses and monitoring strategies when completing a comprehensive risk assessment for the IoT network. The chapter should also provide risk mitigation strategies for each of the identified risks in the five examples: Connected Vehicle IoT, Consumer IoT, Health IoT, Smart Buildings, and Smart Manufacturing. This will help the reader develop a more secure IoT network.
7		Editorial	1382	Misspelling	tornados -> tornadoes
8		Minor	1486	"strong" may be ambiguous	Instead of " strong and" -> should use "secure and"
9		Minor	1486	Many consumer IoT devices are not secure "out of the box"	Add language discussing the need for "out of the box" security, i.e. forced password changes, so that devices are secure on first use.
10		Editorial	1544	Become consistent with previous chart	Change "Health IoT" to "Health IoT systems", to be consistent with previous Consumer IoT chart.

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)
11		Minor	1577	Usually seen as "CIA"	Swap places of Availability and integrity, so the chart headings are "C I A" instead of "C A I"
12		Minor	1581	Users are hesitant to update a working device just for security issues	Consider adding the difficulty in updating a life-preserving device (heart pacemaker, etc)
13		Editorial	1625 - 1627	Consistent bulleted list linked by semicolons.	Remove "and" from last part of line 1625, add "; and" to last part of line 1627
14		Editorial	1633	Grammar	This includes processed -> This includes information processed