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)
	Executive Summary/ Introduction	General Comment		NIST needs to be clearer about what is in each of the sections in the document.	Include an explanation of the layout of the document (e.g. Section 8 will have information about market impact and/or gaps and Section 10 will collect all of the recommendations).
	Section 4	General Comment	Line 159 Page 6	The text states that "market impacts of existing standards are noted and possible gaps in standards identified."	Clarify that the market impacts and the possible gaps are provided in Section 8: Standards Landscape for IoT Cybersecurity of the document. That statement does not appear until page 64, lines 2009-2010 of the Conclusions.
	Section 6	General Comment	Line 762 Page 22	Section 6 is apparently laid out in the same order as Annex D the relationship between Section 6 and Annex is not apparent.	Assuming the relationship between Section 6 and Annex D is correct, insert language to clarify that at the beginning of Section 6, prior to the details provided in Section 6.1.
	Sections 5 and 7 Sections 6 and 8	General Comment		Sections 5 and 7, and Section 6 and 8, are logically associated.	Combine the two sections (Sections 5 and 7, and Sections 6 and 8) to streamline the document and combine ideas that are similar and related.
	Section 9	General Comment		The order of the Core Areas of Cybersecurity Standardization is out of sync with Annex D.	Re-organization to sync with Annex D.
	Annex A	General Comment			Provide a grid with the source of the definition spelled out so that the reader can easily scan the content for differences in interpretation.

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)
	Annex D	Editorial Major		• Notes are included in the description that would be better moved to the discussion in Sections 5 and 7. • Once moved, it might be easier to track which standards impact which Core Area of Cybersecurity if re-arranged (e.g. the standards are listed for each row, with the columns of the Core Area of Cybersecurity and a mark indicating inclusion in a core area). This would also reduce redundant standard entries (e.g. HITRUST is listed multiple times) and will facilitate the analysis/review for impact of a particular standard. • NOTE that the same concept could be applied to the Maturity Level (e.g. ISO/IEC 15408-3:2008 has 5 maturity levels listed). • Missing standards include: OAuth2 (RFC 6749 and 6750) for Identity and Access Management, and several of the HL7 standards (e.g. LH7 Healthcare Privacy and Security Classification System (HCS), Release 1) are not included. Also, HL7 PASS and SLS are two standards, not one. • RFC 4347-2006 has been obsoleted by RFC 6347. • Understanding that draft-ietf-tls-tls13-22 is pending publication, should RFC 5246 (The Transport Layer Security (TLS) Protocol Version 1.2) be provided?	• Move the notes to the other section(s). • Simplify Annex D presentation in a grid/matrix format. • Update for missing standards. • Correct HL7 PASS:SLS entry to reflect two separate standards. • Remove RFC4347-2006 and replace with RFC 6347, which has been updated by RFC 5746 and 7507. • Include RFC 5246 until obsoleted by draft-ietf-tls-tls13-22.
	Annex E	Editorial Major		There is no mapping provided between the NIST references and the Core Areas of Cybersecurity for IoT.	Provide the mapping.
	Annex F	Editorial Minor	Line 2322 Page 173	Missing acronyms for TIR, which is the AAMI acronym for Technical Report –TIR and TR appear to be used interchangeably in various places (and only one should be used for AAMI). Also, 80001 is listed as a "TIR" in some places, "TR" or "AAMI ISO" in others.	Include TIR: Technical Information Report in Annex F. Correctly refer to IEC 80001-1:2010 (e.g., from Annex D)
	Multiple	General Comment	Lines 1773 – 1967	These sections highlight that gaps exist in available international standards integrating IoT, and those standards are either slow to evolve or are non-existent. IoT security may be out of compliance in some areas as well as exposed to higher risks in others.	Add a section that highlights the alignment of this document with the efforts of DHS and HHS to address IoT cybersecurity. Develop a process diagram outlining how this document will be maintained and refreshed.
		Editorial Minor	Line 677	Typo	Change "lower" to "raise"

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)
		General Comment	Section 6, 7	While Annex D covers various cybersecurity topic areas (e.g., identity and access management), it would be good to have more information on how to apply controls from major control frameworks for various IoT Scenarios. Examples of these controls could be taken from major frameworks (e.g., NIST SP 800-53 and ISO 27002), highlighting the differences between these frameworks. This addition would make the document more relevant by showing applications of controls to real-world scenarios that have new attack surfaces. Given limitations in the ability to implement controls some of these scenarios, alternative approaches should also be discussed in Section 7 (e.g., network segmentation, etc.).	First, frame the control discussion by expanding on the 5 IoT scenarios to provide details where controls could be illustrated, related to encryption, identity and access management, etc. Then, for each of the cybersecurity areas (e.g., cryptography, identity and access management, etc.), provide examples of how controls from major frameworks would apply to the IoT scenarios. These examples should highlight the way that IoT affects concepts like the information system "authorization boundary" that is used by NIST SP 800-53 and the "ISMS" that is used by ISO 27001.