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					
2	Industrial Internet Consortium Security Working Group (IIC SWG) iic-security-wg@workspace.iiconsortium.org <iic-security-wg@workspace.iiconsortium.org>	Major	P. 176, 2230-31, and P 66, 2076	The topic of security is treated in isolation, independent of interrelated characteristics of IOT such as safety, reliability, resilience, and privacy, as documented in NIST CPS. NIST is driving the concept of Trustworthiness which includes security, but positions it as part of a system, and should build upon other internal NIST special publications such as 800-160 Volume 1 and draft Volume 2. Annex A references CPS, which addresses a system-wide approach to security, which more accurately describes the IOT landscape.	Taking a cybersecurity-only approach contradicts the results of other NIST documents and adds further confusion around IoT Security. Update the definitions on p. 66 to include the industrial perspective to ensure that the industrial folks adopt the 8200. Apply the learnings of 800-160 and 800-82r2 in this document.
3	Industrial Internet Consortium Security Working Group (IIC SWG) iic-security-wg@workspace.iiconsortium.org <iic-security-wg@workspace.iiconsortium.org>	Minor	1704-1707	While we like the direction this is taking, it is not clear how one can “fail secure”. When talking about IIoT, failing safe is the mandate, and “failing secure” should address resilience, but this is not discussed. Safety has historically superseded all other considerations, and reliability has been a top concern, however, the 8200 considers security as primary, which doesn’t seem to match the reality of the industry. This needs to be considered to make 8200 relevant and to be adopted as part of the IT/OT convergence.	The three primary considerations in industrial sectors are safety, reliability, and security, and these cannot arbitrarily mandate “fail secure” only. A system must fail reliably to a safe state with resilient security still intact. All three must be present for an industrial system to remain operational.

4	Industrial Internet Consortium Security Working Group (IIC SWG) iic-security-wg@workspace.iiconsortium.org <iic-security-wg@workspace.iiconsortium.org>	Minor	Section 7.1	In Ch. 5 the IoT verticals are introduced with some use cases to illustrate some of the primary considerations in each. Then in ch7, a risk-based evaluation of each is provided. However, the document doesn't address why the risk differs in each vertical, which isn't only related to security, and should address the safety, reliability, etc. concerns to fill this gap.	Address each of the verticals in Ch 5 and Ch 7 with the considerations that are important to them. Applying the safety, reliability, and security considerations to these verticals would illustrate the differences in the security impact on each. It would also reinforce the consistent handling of the verticals' risk posture. In each subsection in Ch. 5, discuss the safety, reliability, etc. considerations of each vertical and then address how the security considerations should be handled based on risk in Ch. 7.
5	Industrial Internet Consortium Security Working Group (IIC SWG) iic-security-wg@workspace.iiconsortium.org <iic-security-wg@workspace.iiconsortium.org>	Major	line 288	The document appears to address consumer IoT and apply the concepts to Industrial IoT. The scope appears to address safety and privacy in terms of PII, however, for industrial concerns, privacy is not (yet) a driving consideration. The driving forces in IIOT are safety, reliability, and security as the primary triad. This is not addressed in the scope section. Safety is referenced 38 times, which may be appropriate for IIoT. Reliability is referenced 5 times, which is very low for IIoT. Resilience is referenced 21 times. Security is referenced 1000+ times (since it's a security paper) Privacy is referenced 57 times which is likely very appropriate for consumer IoT, but is likely not a top priory (yet) in all of the Industrial verticals. The scope is too narrow to accurately address security for the intended audience (International cybersecurity body) as there is too much of the traditional isolationist treatment of security.	Perhaps including the perspectives of 800-82 to provide a more complete discussion related to the role of security in IoT within industrial verticals would help illustrate the challenges of working with security when the primary drivers are safety and reliability. Adding IoT to these verticals creates further challenges to properly addressing risk (not just security risk) and this should be addressed thoroughly. Page 1, Executive Summary of 800-82r2 (2015) clearly outlines that security cannot be separated from the industrial considerations of safety and reliability in a meaningful way. The 8200 would greatly benefit from extending the 800-82 perspective into the realm of IoT (IIoT).

6	Industrial Internet Consortium Security Working Group (IIC SWG) iic-security-wg@workspace.iiconsortium.org <iic-security-wg@workspace.iiconsortium.org>	Minor		What is the target audience for this document? Consumer? Industrial? There are very different considerations between those sectors of IoT, so it is difficult to comprehensively cover them without addressing each in turn. The paper must either choose a narrower perspective, or else expand the scope and discuss each aspect in more detail. Is this targeting Govt? There is very little OT in government, so applying same techniques to medical as one applies to consumer leads to vastly different risk. Vastly different risk is addressed with different security approaches, so generalizing becomes suspect in these types of documents. The closer you get to industrial, the less relevant this document becomes.	Please define the audience and how you expect them to use this document in practice.
7	Industrial Internet Consortium Security Working Group (IIC SWG) iic-security-wg@workspace.iiconsortium.org <iic-security-wg@workspace.iiconsortium.org>	Minor	Line 346-7	Data storage is part of the IOT Component. Should be part of the IoT System or Environment	Data storage is critical to IoT. However, requiring data storage (as defined in section starting line 397) on each IoT Component doesn't make sense. A sensor shouldn't need to store the data over time. Something in the IoT System or the IoT Environment should provide this function, but not be a required element in the component (which is how we're interpreting this).

8	Industrial Internet Consortium Security Working Group (IIC SWG) iic-security-wg@workspace.iiconsortium.org <iic-security-wg@workspace.iiconsortium.org>	minor	P34	The diagram looks like someone took 4 diagrams, put them in a blender, and dumped the results on the page. There is a lot going on in this diagram, and it needs more description to explain what is going on.	Really like the diagram but have no idea what it's trying to communicate. Either explain it or cut it.
9	Industrial Internet Consortium Security Working Group (IIC SWG) iic-security-wg@workspace.iiconsortium.org <iic-security-wg@workspace.iiconsortium.org>	minor	Line 2179, page 107	Section Annex D tables for IT System Security Evaluation should list IIC activities related to the IIoT Endpoint Security Best Practices, IoT Security Maturity Model, Key Safety Challenges for the IIoT, and the Industrial Internet Security Framework, which are all relevant to the topics treated in this document.	Insert a new row mentioning IIC and pointing to the initial IIC An accompanying practitioner's guide will be published aroun
10	Industrial Internet Consortium Security Working Group (IIC SWG) iic-security-wg@workspace.iiconsortium.org <iic-security-wg@workspace.iiconsortium.org>	minor	Line 1267	Medical devices prioritize integrity over the others since it relates most strongly to patient safety.	Don't disagree with the point you're trying to make, but this is a completely unsupported claim. Please provide reference or at least some supporting logic to explain this overlap between safety and security. This is where trustworthiness can be a lever to explain that these overlaps are natural in industrial, and that integrity can have impact on both safety and security. However, you'd still need to refactor that statement as there is no clear mapping between integrity (security) and safety.

11	Industrial Internet Consortium Security Working Group (IIC SWG) iic-security-wg@workspace.iiconsortium.org <iic-security-wg@workspace.iiconsortium.org>	Minor	Page 157	Would you consider adding the following to the list of System Security Engineering if IoT Blockchain is within the scope of the 8200 document: P2418 - Standard for the Framework of Blockchain Use in Internet if Things (IoT)	P2418 - Standard for the Framework of Blockchain Use in Internet if Things (IoT) IEEE P2418 standards.ieee.org/develop/project/2418.html Status: Under Development