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	Schrecker, Sven <sven.schrecker@intel.com>	Editorial	Line 280	these networked connected devices need to be secure and resilient.	Should be “network connected”
2	Schrecker, Sven <sven.schrecker@intel.com>	Editorial	Line 341	Definition of IoT Component: A type of component that can be composed into IoT systems Very awkward sentence. Perhaps it’s more intuitive to say: “IoT Systems can be decomposed into IoT Components” or “IoT Components make up IoT Systems”.	“IoT Systems can be decomposed into IoT Components” or “IoT Components make up IoT Systems”
3	Schrecker, Sven <sven.schrecker@intel.com>	major	Line 379	It isn’t clear why there are primary and secondary capabilities. What makes the primary ones primary? Why are the rest secondary? This is never explained. I understand that networking and processing are required be EVERY IoT Component. Those should be primary. I understand that some IoT Components may have sensing and actuating. Those could be secondary (or optional?) capabilities. My gateway is an IoT device because it has some of the capabilities listed (but it’s unlikely any IoT device will have ALL of the “primary” capabilities in every device). Data storing? My little temp sensor doesn’t have enough capability to do much data storage. Therefore, it’s not an IoT Component? That doesn’t sound right. Data Storing has to be addressed somewhere in the IoT System, or even the IoT Environment, but is not Primary on each IoT component.	Make networking and processing the definition of IoT Component (aligned with NIST vocabulary document) Define sensing and actuating as optional capabilities. Remove data storing as a capability of an IoT Component and place elsewhere unless we’re unclear on the definition of an IoT Component. You can add the HUI and Supporting (??) capabilities as optional as well.
4	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 379	why have networking and network interface as two different capabilities? They’re not independent. (See comment for line 436 below) How can you do networking without some sort of network interface? Perhaps you mean something specific by “network interface” which is defined as “an Ethernet Card”, but we’re imagining a wired or wireless interface to some communications medium is also a “network interface”. Does that make sense?	Use either Networking primary capability and get rid of the requirement to have an ethernet card as wireless interfaces are much more prevalent.

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)
5	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 383-384	"Using this capabilities viewpoint, an IoT component can be understood by the set of capabilities it provides." Using "this capabilities" is a little awkward. Consider rewriting it.	Using the Capabilities Viewpoint, an IoT Component can be understood by the set of capabilities it provides.
6	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 383-384	"Using this capabilities viewpoint, an IoT component can be understood by the set of capabilities it provides." awkward. Who is doing the understanding?	One can understand the set of capabilities provided by an IoT component using the capabilities viewpoint.
7	Schrecker, Sven <sven.schrecker@intel.com>	editorial	Line 394	cardiac pacing and electric shock delivery are reversed. It appears (to us) from the context of the other examples that the format follows this pattern: Desired outcome (physical action) Therefore, the electric shock delivery example is backwards.	Cardiac pacing (electric shock delivery)
8	Schrecker, Sven <sven.schrecker@intel.com>	major	Line 398	Data storage may not be part of every IoT component, but rather part of the IoT system. This is different from fundamental capabilities such as networking capability	Remove the requirement for data storage to be an IoT component. There is no feasible requirement for a tiny sensor (door sensor, light sensor, etc.) which just has 1/0 state to have to store any data for any length of time. This is more applicable to an IoT System, so that there is some IoT Component that performs the function of Data Storage (and likely aggregation, correlation, and analytics as well), but not every IoT component.
9	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 409	processing is not necessarily transforming data. Processing is a systematic series of actions directed towards an end. What's described here is not "processing".	Fix definition of processing: Processing is a systematic series of actions directed towards an end.
10	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 413	"These control algorithms often are used within negative feedback loops, but not always. A proportional-integral-derivative (PID) control algorithm is an example of such a control algorithm." This is a bit of an obscure example. Can you please provide an example that most practitioners can relate to??? Thanks.	Please explain the relevance of the example to IoT and security. I'm not clear what this example means and therefore why it's relevant, so perhaps you could clarify. Apologies if one should know the PID algorithm and I simply don't.
11	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 436	each IoT component must have at least one network interface YES! So why not just make the processing and networking (or interface) mandatory? Really convoluted right now.	Clearly define what you mean by network interface (opaque at the moment), or else just get rid of it and stick with networking as primary

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
12	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 442	"Supporting" is not the right word to describe authentication and cryptographic functionality. If there are other functions, then list them, otherwise, this is not a clear description of a "secondary" capability of an IoT Component.	Rename or redefine "supporting"
13	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 442	supporting capability is not the same granularity as network interface and user interface. The other two capabilities are clear and descriptive, but "supporting" seems to be a catch-all bucket with broad reach. Perhaps identifying/enumerating the elements within that category would help.	Rename or redefine "supporting" Perhaps you can add additional examples such as: • system memory encryption • trusted execution and trusted execution environment
14	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 446	risk-adjacent- What is "risk-adjacent-" ???	Refactor the sentence to clarify or else define the term for us
15	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 447	"IoT components performing sensing and/or actuating capabilities do not normally incorporate cryptographic controls (i.e. supporting capability) built-in so risk-adjacent-authentication is difficult unless additional engineering is implemented" Not sure that's a consistent perspective in the industry. Please be concise and clear on this point because it's critical to the paper. We shouldn't say that sensing and actuation normally doesn't include encryption without explaining why or describing why it may be important in some cases?	Replace the blanket statement that most IoT Components don't incorporate crypto with one stating that they should, why they currently don't, and that there are other (existing) options to implement the crypto (gateways, et. al.).
16	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 449	is this related to security? Agree with the statement, but no tie-in is provided.	We don't dislike this section, but it's not clear how it's tied in to security. Explain?
17	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 541	"The proper implementation of security within consumer IoT software, firmware, and hardware is often a neglected and overlooked priority. Securing IoT devices is a major challenge, manufacturers tend to focus on functionality, compatibility requirements, and time-to-market than security. " Finally! First mention of inadequate security in IoT, as well as a (short) explanation of why this is the case.	Can you address this point much earlier in the document? Maybe it's considered obvious, but then why add it here? Please consider making this important statement right off the bat at the start of the document.

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
18	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 571	Section 5.3, healthcare, is unlike the other sections. It deals almost exclusively with humans. It's clear that health care doesn't exist without the human, but the topic is IoT Security, and that's not touched upon as it is in the other sections	Consider adding some concrete technology examples: insulin pump, etc.
19	Schrecker, Sven <sven.schrecker@intel.com>	major	Line 468-761	There doesn't appear to be any sort of consistent format within these subsections (5.1-5.5) In some cases, there are tables, in other cases just diagrams, but the content is all over the board. It would be very helpful to provide a consistent layout for these sections: safety considerations of the vertical: security considerations, privacy considerations, reliability, resilience. This would juxtapose the verticals more clearly. E.g. Consumer IoT has different safety and reliability considerations than automotive (also includes privacy), which are again different from health IoT (maximum privacy)	See if there isn't a consistent format that can be applied to normalize the sections 5.1-5.5
20	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 579	Characteristics of the Health IoT Environment This section only has 2 sentences and a table.	Explain something insightful or consider cutting it
21	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 586	entire healthcare subsection is use cases. Very little technology	Revise to include some technology (see prior comment regarding consistent format of these subsections)
22	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 656	Does this table imply that managers are IoT components? The tables are confusing and unclear	Clarify the table title and spell out what each should be communicating to the reader. It may help to have consistent format across these subsections in Ch. 5.
23	Schrecker, Sven <sven.schrecker@intel.com>	editorial	Line 676	"After a while, several users begin to complain that it is too cold. Individually, they open the building control app and submits their request to **lower** the temp in their area and increase the lighting. " Oops!!!	Reverse the example... people don't ask for the temp to be lowered if it's too cold 8^)

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
24	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 646	smart buildings subsection in Ch. 5 is one paragraph, a table, and one long use case story	Clarify the table purpose and spell out what each should be communicating to the reader. It may help to have consistent format across these subsections in Ch. 5.
25	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 695	second mention of "better security needed in industrial". Another revelation where the reader has to go all the way to page 19. Perhaps this should be introduced earlier in the document since it seems to be a critical point?	Mention this much earlier in the document. Also, these sections in Ch. 5 appear to come from different authors, which is fine for this point in the evolution of the document, but the editors should ensure the text has a consistent level of detail and format as well as consistent set of views on the issues throughout the document.
26	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 700	YES! This is a good structure for sections in Ch. 5. All sections should be structured more like this with relevant content that explains what is needed, why it's important, and what steps must be taken.	Please revise the other sections to mimic the format, content, and level of detail (specificity) of subsection 5.5, which is quite clear and concise
27	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 718	first mention of IT/OT convergence	This is a critical element to the IIoT verticals, but the first mention is on page 20. Make this point earlier in the document and consider discussing the considerations of IoT on Industrial Verticals (i.e. Trustworhiness) there as well.
28	Schrecker, Sven <sven.schrecker@intel.com>	editorial	Line 727	"For example, a 3D printer file may need not only to be encrypted security, but also may require provisions to restrict the number of allowable uses. " unclear sentence -requires encryption and access control to limit number of allowable uses. Did you mean users? I suspect encryption may needed, but where? The current sentence seems to indicate that you need to encrypt the 3D printer file and limit the number of times that it can be printed. Is that the right interpretation? Perhaps integrity is sufficient in some cases?	For example, a 3D printer must restrict the number of allowable times that each encrypted/signed data file may be printed out. Sorry if we missed the meaning of this sentence.
29	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 751	calls out related standard/profile. Do this in all sections	This is really useful. Can you do this in other sections? May be a key to successful adoption of this document.

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
30	Schrecker, Sven <sven.schrecker@intel.com>	editorial	Line 766	trust-worthy - one word?	I believe NIST spells it “trustworthy” in other documents. Not critical but should be consistent.
31	Schrecker, Sven <sven.schrecker@intel.com>; Quaranta, James R <james.r.quaranta@intel.com>	Minor	Section 6.1	Cryptographic Techniques: There are several techniques that we consider to be critical to IoT and IIoT: • Anonymous Attestation o ISO/IEC 20008-1:2013 – Part 1: General • Anonymous Digital Signatures o ISO/IEC 20008-2:2013– Part 2: Mechanisms using a group public key • Anonymous Entity Authentication – Part 1: General o ISO/IEC 20009-1:2013 • Anonymous Entity Authentication – Part 2: Mechanisms based on signatures using a group public key o ISO/IEC 20009-2:2013 • Anonymous entity authentication -- Part 3: Mechanisms based on blind signatures concepts o ISO/IEC 20009-3 [under development] • Anonymous entity authentication -- Part 4: Mechanisms based on weak secrets o ISO/IEC 20009-4:2017	Please add these techniques to Section 6.1 as they are extremely valuable to IoT and IIoT.
32	Schrecker, Sven <sven.schrecker@intel.com>	editorial	Line 767	There is a fair amount of detail here, which is good. It’s not clear what level of experience the reader will have, so it may be good to explain the difference between entity auth and message auth. It’s implicit in the following paragraphs, but not explicitly stated even though it’s explicitly called out on line 767	Explain entity auth and message auth explicitly or else remove the explicit reference on line 767
33	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 771-780	Good opportunity to explicitly map these concepts to the statement in 764-767	Consider explaining the statement in 764-767 in this bullet list more clearly

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
34	Schrecker, Sven <sven.schrecker@intel.com>	editorial	Line 784	which are a digital signatures	Remove the “a” or remove the “s”
35	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 785-786	“Encryption provides confidentiality to data at rest and in transmission. “ One other consideration that is sometimes raised is protecting “data in use”. There are multiple places in the document where this could be addressed.	also add “data in use” in addition to “data in transit” (transmission) and “data at rest”
36	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 789	Cryptographic techniques do not directly provide availability; on the other hand, poor implementations of cryptographic techniques can significantly decrease availability of communication networks. “ Can you explain how do poor crypto decrease availability?	Unsubstantiated. Please provide reference or explain.
37	Schrecker, Sven <sven.schrecker@intel.com>	editorial	Line 801	use abbrev IETF since you introduced the abbreviation in previous paragraph	The abbreviation only needs to be defined once, and it was defined in the previous paragraph.
38	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 814	Good format, very understandable. Can you please use this format for 801?	Reformat elements starting on line 801 in a bullet list similar to the ones on 814?
39	Schrecker, Sven <sven.schrecker@intel.com>	editorial	Line 831	in in	in
40	Schrecker, Sven <sven.schrecker@intel.com>	minor	Line 1236-1239	Cybersecurity is as the prevention of damage to, unauthorized use of, exploitation of, and—if needed—restoration of electronic information and communications systems, and the information they, in order to strengthen the confidentiality, integrity and availability of these systems	Can we define this much earlier in the paper instead of on page 33?

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
41	Schrecker, Sven <sven.schrecker@intel.com>; Quaranta, James R <james.r.quaranta@intel.com>	major	Section 7	There seems to be a missing aspect related to the ability to encrypt the system memory and having trusted execution (e.g. TEE) capability. There are many (many, many, many) who consider these to be critical elements of IoT and therefore should be included in this document.	Please discuss system memory encryption Please discuss trusted execution and trusted execution environment As capabilities of the IoT Component (perhaps in Ch. 4? It may also make sense in “Supporting Section” (lines 442-447))