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	IDmachines	Major	293	Confusion between information security and cybersecurity. The language does not match the diagram. It talks about cybersecurity standards in the paragraph and then information security standards in the diagram.	"cybersecurity standards need to be sure to apply information security best practices and standards to ensure confidentiality, integrity, or availability of personally identifiable information (PII) to fully protect individuals' PII.
2	IDmachines	Major	300	Privacy concern arise from byproduct of unauthorized as well as authorized PII processing	"arise from PII processing and byproducts"
3	IDmachines	Major	300	Security concerns can also occur from authorized but inappropriate system behavior. A number of recent examples resulted from authorized behavior (e.g. a signed EULA) with bad outcomes.	"arise from improper system behavior"
4	IDmachines	Major	344-386	The IoT component definition is confusing. It states it provides a network interface, this does not allow a separation of sensors and networking devices. For example, is an analog output a network interface? Further the system definition is not any different that the component definition except there are multiple units. Further the IoT System definition is also odd particularly in the case in figure 2 where the IoT Component is a system.	Not sure how to handle this, I suggest eliminating environment and having system be top level and comprised of components that include sensors/actuators, networking and interfaces. The arrows on Figure are incorrect in several cases. The UI and Network Interface should be bi-directional. Actuation is an output while sensing is an input, networking capability can be both but not necessarily, processing capability is bidirectional, perhaps call out IoT Components (plural) and reference to the capabilities as components.
5	IDmachines	Minor	400	Patient data versus patient records would be more appropriate. There is no reason to store records in IoT components particularly in Figure 2. Data minimization is an crucial design element particularly in healthcare and this might encourage storage when not necessary.	"Electronic patient data is an example of this."
6	IDmachines	Minor	405	RS-422 is a specific serial protocol, if you use ethernet as a general category then use serial communications or include (RS-232 and RS-485)	"serial communications or (RS-232, RS-422 and RS-485)"
7	IDmachines	Minor	406	I don't get the haptic robot example for networking, actually some of this is a sensor feedback through the haptic user interfaces. By using this example, you confuse user interfaces and networking.	Find another example.
8	IDmachines	Minor	408	Some mention and perhaps a differentiation between signal processor and data processing. Signal process plays an important role and is not covered here of in sensing below.	Final a place to include signal processing as an example.
9	IDmachines	Minor	422	Analogue is not the preferred spelling.	analog
10	IDmachines	Minor	423	A switch is not a sensor, for a example a light sensor can trigger a switch and the description differentiates between them.	Use a digital thermometer as an example.

11	IDmachines	Minor	445	Confusion between IoT Components and Components, IoT components should authenticate and encrypt as they include network communications while the sensing or actuations entities that are components do not.	"Components performing sensor and/or actuating….
12	IDmachines	Minor	472	DSRC has been around since 1999, while it is true it is still being studied the reference makes this seem like it is a new thing.	Offer a reference with background on DSRC. The other reference refer to specifics of this such as credential management an overarching example would be useful.
13	IDmachines	Minor	497	The drawing shows a number of communications directly with a certificate authority. Chain of trust and certificate validation typically takes place via a certificate revocation list, or other validation techniques. Also it would be more accurate to say the device sends a certificate request than to say it sends a public key, if in fact this is the case. Give the note about the privacy and security challenges inherent in that architecture, I worry about the side effect of this being adopted as drawn.	Add picture of certificate validation endpoint, change language to say generates certificate request.
14	IDmachines	Minor	Figure 5	It shows HTTP over TLS, should this be HTTPS, HTTP over TLS is a rather old RFC (2818) and has been superceded.	If appropriate show an HTTPS connection.
15	IDmachines	Minor	1593	One of the major weaknesses that exist in physical security systems are physical access control systems that use weak credentials one-way open communications between card readers and door controllers. The Security Industry Association, and ANSI SDO has developed the Open Supervised Device Protocol (OSDSP) https://www.securityindustry.org/industry-standards/open-supervised-device-protocol/ which is currently undergoing wide industry adoption. It mitigates a number of important physical security threats and since physical security plays an important role in a overall information security profile, it mitigates threats across deployments and systems.	Include an OSDP reference
16	IDmachines	Minor	1989	Include SIA as relevant SDO particularly for smart buildings	Include SIA as relevant SDO under cryptographic techniques or under Network Security as the card reader to door controller is a critical network link in smart buildings and the current categorization shows standards needed.
17	IDmachines	Major	2165	Include OSDP as standards reference	Show OSDP, use above link, Security Industry Association as SDO, Guidance Available, Commercial Available, Market Acceptance and Reference Implementation, Notes: Open Supervised Device Protocol (OSDP) is an access control communications standard developed by the Security Industry Association (SIA) to improve interoperability among access control and security products. OSDP v2.1.7 is currently in-process to become a standard recognized by the American National Standards Institute (ANSI), and OSDP is in constant refinement to retain its industry-leading position

February 12, 2018

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