**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 | Anna Johnston, Principal Engineer, Juniper Networks, Sunnyvale, CA | Minor | Page 4, lines 317-318 | The draft NISTIR claims that information resources would be IoT, but the IoT related to information would be a server or other data storage device. In addition, the draft NISTIR identifies people as IoT, but the IoT with respect to a person would be a sensor or actuator connected to a person. | Replace "information resources" with "data storage device."<br><br>Delete "people." |
| 2 | Anna Johnston, Principal Engineer, Juniper Networks, Sunnyvale, CA | Minor | Page 6, line 387 | Separate IoT component, which has a very wide range of capabilities and functions, and IoT system, which is the heart of IoT. | Delete "(which may also be an IoT system)" |
| 3 | Anna Johnston, Principal Engineer, Juniper Networks, Sunnyvale, CA | Major | Page 22, lines 764-791 | The draft does not define 'user.' Also, the pillars of security are not recognized as industry standards and some of them overlap. | Replace with:<br><br>Cryptographic techniques are indispensable in securing IoT data and transactions. Implementation of such techniques provides information assurance, which is built upon the following objectives of cybersecurity:<br><br>1. System Access: Access control by verifying a user's identity and level (administrative, read only, or other more detailed levels). A users access should be restricted to only those levels they have privileges for.<br><br>2.Data Integrity: Data integrity insures availability of the data in its original form. Unauthorized modifications, including deletion, should be protected against. The data should be available to authorized users as needed. Data authentication – being able to show that data was produced from a given entity or set of entities -- can be considered a part of data integrity. Electronic signatures, which enable non-repudiation if the social enforcement is available, are a subcategory of data authentication<br><br>3. Data Confidentiality: Data should remain confidential to all but authorized users. Also called 'privacy', and generally involves encryption.<br><br>When considering these pillars, users can be defined as individual persons, entities, or processes that require access or connections to IoT device or system. |

| **COMMENT #** | **SOURCE** | **TYPE i.e., Editorial Minor Major** | **LINE # PAGE etc.** | **RATIONALE for CHANGE** | **PROPOSED CHANGE (specific replacement text, figure, etc. is required)** |
|---|---|---|---|---|---|
| | | | | | |
| 4 | Rosa Underwood, Senior Systems Engineer, Juniper Networks, Herndon, VA | Minor | Page 26, line 948 | Information Security Management Systems (ISMS) are a subset of processes and controls instead of, as the draft NISTIR implies, an umbrella process or control. | Replace “provide a set of” with “serve as a component of.” |
| 5 | Rosa Underwood, Senior Systems Engineer, Juniper Networks, Herndon, VA | Editorial | Page 28, line 1051 | Awkward word choice. | Replace “over” with “using.” |
| 6 | Rosa Underwood, Senior Systems Engineer, Juniper Networks, Herndon, VA | Editorial | Page 28, line 1067 | The sentence (“Many standards developers have developed and are developing network security standards.”) might not convey the intended concept that there is a multitude of entities engaged in standards development. The sentence can be read to say, in a circular manner, that many standards developers are developing standards. | Replace the sentence with “A variety of organizations are involved in developing network security standards.” |
| 7 | Rosa Underwood, Senior Systems Engineer, Juniper Networks, Herndon, VA | Minor | Page 30, line 1152 | The list of relevant software assurance standards in 6.9 is incomplete. | Add OWASP Secure Software Development Lifecycle as a relevant standard. |

| COMMENT # | SOURCE | TYPE i.e., Editorial Minor Major | LINE # PAGE etc. | RATIONALE for CHANGE | PROPOSED CHANGE (specific replacement text, figure, etc. is required) |
|---|---|---|---|---|---|
| 8 | Anna Johnston, Principal Engineer, Juniper Networks, Sunnyvale, CA | Major | Page 33, Lines 1245-1249 | The cybersecurity objectives should match the pillars of security from section 6. | Replace with:<br>1. System Access: Access control by verifying a user's identity and level (administrative, read only, or other more detailed levels). A users access should be restricted to only those levels they have privileges for.<br>2.Data Integrity: Data integrity insures availability of the data in its original form. Unauthorized modifications, including deletion, should be protected against. The data should be available to authorized users as needed. Data authentication – being able to show that data was produced from a given entity or set of entities -- can be considered a part of data integrity. Electronic signatures, which enable non-repudiation if the social enforcement is available, are a subcategory of data authentication<br>3. Data Confidentiality: Data should remain confidential to all but authorized users. Also called 'privacy', and generally involves encryption. |
| 9 | Rosa Underwood, Senior Systems Engineer, Juniper Networks, Herndon, VA | Minor | Page 33, lines 1251-1254 | The NISTIR displays acceptance of the slow pace it takes to develop and approve standards, and thus it should highlight the critical need for a faster cadence in order to facilitate strong IoT cybersecurity. | Add as a new sentence at the end of line 1252: "Timely development of standards is a component of mitigating risks." |
| 10 | Rosa Underwood, Senior Systems Engineer, Juniper Networks, Herndon, VA | Editorial | Page 33, line 1254 | "Availability" misspelled as "availably." | Replace "availably" with "availability." |

| COMMENT # | SOURCE | TYPE i.e., Editorial Minor Major | LINE # PAGE etc. | RATIONALE for CHANGE | PROPOSED CHANGE (specific replacement text, figure, etc. is required) |
|---|---|---|---|---|---|
| 11 | Rosa Underwood, Senior Systems Engineer, Juniper Networks, Herndon, VA | Minor | Page 33, lines 1259-1262 | These lines contain a definition of IoT that, in some ways, contradicts or diverges from the definitions contained in section 4 and in Annex A. For example, IoT does NOT consist of “the facilities.” While facilities such as security operations centers (SOCs), office buildings, etc. contain IoT devices, the approach to security is much different and thus should not be considered IoT. This definition does not add substantive value to the section and thus can be deleted. | Delete lines 1259-1262. |
| 12 | Rosa Underwood, Senior Systems Engineer, Juniper Networks, Herndon, VA | Minor | Page 34, lines 1277-1278 | The sentence (“Medical devices prioritize integrity over the others since it relates most strongly to patient safety.”) states as fact what actually is the NISTIR author’s opinion. Absent contradictory data from relevant sources, it is possible to say that some providers or patients consider availability or confidentiality as higher priorities for medical devices. | Either (1) delete the sentence that begins on line 1277 and ends on line 1278 or (2) provide a citation to another source so that it is the opinion of the author. |
| 13 | Rosa Underwood, Senior Systems Engineer, Juniper Networks, Herndon, VA | Editorial | Page 35, lines 1286-1288 | The sentence on mitigating system vulnerability is redundant with the preceding sentence. | Delete the sentence that begins on line 1286 and ends on line 1288. |
| 14 | Rosa Underwood, Senior Systems Engineer, Juniper Networks, Herndon, VA | Minor | Page 35, lines 1312-1313 | Providing unauthorized modification of data as a security objective would benefit from additional explanation. | Add as a new sentence at the end of line 1313: “Methods such as encryption and digital signatures can be used to preserve the integrity of data.” |

| COMMENT # | SOURCE | TYPE i.e., Editorial Minor Major | LINE # PAGE etc. | RATIONALE for CHANGE | PROPOSED CHANGE (specific replacement text, figure, etc. is required) |
|---|---|---|---|---|---|
| 15 | Rosa Underwood, Senior Systems Engineer, Juniper Networks, Herndon, VA | Minor | Page 40, line 1487 | The draft NISTIR recommends strong passwords, but strong passphrases provide better security. | Replace “passwords” with “passphrases.” |
| 16 | Rosa Underwood, Senior Systems Engineer, Juniper Networks, Herndon, VA | Major | Page 44, lines 1608-1612 | The draft NISTIR states that heterogeneous networks create security challenges. This does not account for the fact that homogeneous networks also can be vulnerable because they can be subject to single points of failure; in that regard, heterogeneous networks can provide security advantages. | Replace the sentences that begin on line 1608 and end on line 1612 with: “The challenges associated with securing smart buildings and their multitude of devices can be mitigated through performing interoperability testing and selecting products placed on Approved Product Lists (APLs) after undergoing testing by accreditation labs.” |
| 17 | Rosa Underwood, Senior Systems Engineer, Juniper Networks, Herndon, VA | Minor | Page 44, lines 1613-1615 | The cybersecurity risks associated with employees, visitors, and their components interacting with building networks can be addressed. | Add as a new sentence at the end of the sentence that ends on line 1615: “Appropriate security policies and security awareness programs, particularly focused on Bring Your Own Device risks, can help mitigate the risk of employee and visitor device interactions with building networks.” |
| 18 | Anna Johnston, Principal Engineer, Juniper Networks, Sunnyvale, CA | Minor | Page 47, lines 1751-1759 | The draft suggests elliptic curve cryptography (ECC) as the choice for public key cryptography. At the same time, there is momentum toward quantum resistant cryptography. Because no currently known quantum resistant algorithms are standardized for use, finite field cryptography might protect against quantum attacks better in the meantime. This is because quantum attacks on ECC, finite field based cryptography, and RSA are based on the group size. The group size of elliptic curves is quite limited, while the group size of finite field cryptography has plenty of room for growth and could protect against quantum attacks. | Replace with:<br>Finite field based cryptography could be the best choice for public key cryptography in light of the momentum toward quantum resistant cryptography. None of the currently known quantum resistant algorithms are standardized for use, but finite field could fill the gap in the meantime. This is because quantum attacks on ECC, finite field, and RSA are based upon the group size, and finite field offers room for growth that could better protect against quantum attacks. |

| COMMENT # | SOURCE | TYPE i.e., Editorial Minor Major | LINE # PAGE etc. | RATIONALE for CHANGE | PROPOSED CHANGE (specific replacement text, figure, etc. is required) |
|---|---|---|---|---|---|
| 19 | Rosa Underwood, Senior Systems Engineer, Juniper Networks, Herndon, VA | Minor | Page 48, line 1766 – 1771 | The draft NISTIR states that blockchain is under development even though Bitcoin uses blockchain technology and has been in existence since 2009.<br>In addition, lines 1770-1771 implies, despite evidence to the contrary, that standards organizations are not engaged in developing standards for blockchain. | Expand the phrase on line 1769 from “blockchain is still under development” to “blockchain is still under development for IoT.”<br>On line 1771, replace the phrase “should be taking note” with “have taken note. The International Standards Organization is working to standardize blockchain and Distributed Ledger Technologies (DLT) under ISO/TC 307. |
| 20 | Rosa Underwood, Senior Systems Engineer, Juniper Networks, Herndon, VA | Editorial | Page 48, line 1783-1784 | The statement that “Market implementations are lagging for IoT systems” is not clear. | Please elaborate on what this statement is intend to convey. |