Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

April 18, 2018

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

COMMENT # (21 in total)	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
1	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Major	Line 316-378, pages 4-5	Unclear from the document what the difference is between an IoT system and an IoT environment and how that does or does not fit with cyber-physical systems	Suggest to add more clarification on that question/topic

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

April 18, 2018

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

2	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Major	Annex D, "Cryptographic Techniques", document "TPM", SDO "TCG", page 81-82	Document references TPM 1.2, but the TPM 2.0 standard has been available since 2012, offering support for additional algorithms and capabilities. Recommend revising the reference to the TPM 2.0 standard.	Column: "Documents", replace with "TPM (hyperlink to https://trustedcomputinggroup.org/tpm-library-specification/), September 2016 or later" Column: "Description", replace with " Trusted Platform Module (TPM) 2.0 The TPM 2.0 provides support for a wide array of cryptographic operations including hashing, symmetric and asymmetric encryption, key generation, digital signatures, random number generation, protected storage and protected capabilities. The TPM architecture is cryptographic agile with support for numerous algorithms and curves with an extensible model to add more algorithms or curves as needed. The TPM 2.0 standard uses a library model so simpler profiles for a particular purpose can be defined using a subset of the available algorithms and capabilities to address platform specific requirements or constraints like Mobile, Automotive or IoT. The TPM 2.0 can create Endorsement Keys that serve as a statically unique TPM identity or an identity for an IoT component that a TPM is bound to. TPM manufacturers may also issue Endorsement Key certificates to provide confidence to third parties that interaction with a TPM is based on an implementation provided by the manufacturer issuing the certificate. TPM generated keys can be used for device authentication and cryptographically associated with Endorsement Keys in a TPM. TPM 2.0 supports anonymous remote attestation to help remote entities validate IoT component software measurements stored in a TPM during the boot process or based on the dynamic launch of a measured component. Remote attestation and its local equivalent called sealing provide evidence of IoT component integrity for both code and configuration." Column: "Maturity Level", replace with " Approved Standard Technically Stable Reference Implementation Testing Conformity Assessment Commercial Availability Market Acceptance" Column "Notes", replace with " What is TPM 2.0? An International standard (also published as ISO/IEC 11889:2015) that enables trust in computing platforms in general by receiving commands

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

					and returning responses using protected capabilities that provide hardware roots of trust for storage, measurement and reporting. “
3	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Major	Annex D, "Cryptographic Techniques", document, SDO "TCG", page 82	Recommend adding the new TCG DICE standard for its benefits for device authentication and integrity	Column: “Documents”: “DICE (hyperlink to https://trustedcomputinggroup.org/work-groups/dice-architectures), March 22, 2018” Column: “Description”: “Hardware Requirements for a Device Identifier Composition Engine (DICE) DICE provides foundational security properties for IoT component identity authentication and attestation with extremely minimal hardware requirements making it well suited for constrained devices and IoT components. Each layer of the boot process receives secrets based on a combination of the device identity and the measurements of software code and configuration. The TCG DICE specification defines the platform reset actions and hardware requirements. The TCG Implicit Identity Based Device Attestation Reference document explains how successive software layers can extend the model for each layer and provide evidence of device identity authentication and integrity to remote entities using derived keys, certificate chains and existing protocols like TLS.” Column: “Maturity Level”: “ Guidance Available Reference Implementation” Column “Notes”, replace with “ What is DICE? A combination of an industry standard and a reference document that provide device identity and attestation capabilities with extremely minimal hardware requirements.”

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

April 18, 2018

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

4	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Major	Annex D, "Identity and Access Management", SDO "TCG", page 102	Document references TPM 1.2, but the TPM 2.0 standard has been available since 2012, offering support for additional identity and authentication capabilities. Recommend revising the reference to the TPM 2.0 standard.	Column: “Documents”, replace with "TPM (hyperlink to https://trustedcomputinggroup.org/tpm-library-specification/), September 2016 or later” Column: “Description”, replace with “ Trusted Platform Module (TPM) 2.0 TPM 2.0 provides a root of trust for storage, protecting cryptographic keys used for authentication and authorization from disclosure. Usage of keys can be protected by simple authorization values, dictionary attack logic and/or arbitrarily complex policies involving multiple parties, time and values of nonvolatile protected data. A variety of options exist for protecting communication sessions between software and a TPM and auditing TPM usage. The TPM 2.0 can create Endorsement Keys that serve as a statically unique TPM identity or an identity for an IoT component that a TPM is bound to. TPM manufacturers may also issue Endorsement Key certificates to provide confidence to third parties that interaction with a TPM is based on an implementation provided by the manufacturer issuing the certificate. TPM generated keys can be used for device authentication and cryptographically associated with Endorsement Keys in a TPM.” Column: “Maturity Level”, replace with “ Approved Standard Technically Stable Reference Implementation Testing Conformity Assessment Commercial Availability Market Acceptance” Column “Notes”, replace with “ What is TPM 2.0? An International standard (also published as ISO/IEC 11889:2015) that enables trust in computing platforms in general by receiving commands and returning responses using protected capabilities that provide hardware roots of trust for storage, measurement and reporting. “

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

April 18, 2018

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

5	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Major	Annex D, "Software Assurance"	Add ISO/IEC 27034:2011+ (or ISO/IEC 27034-1:2011 specifically)	NIST should include ISO/IEC 27034-1:2011 in Annex D under “Software Assurance.” This standard is already referenced in line 1132 on page 30, but it should also be included in Annex D because it provides guidance on specifying, designing/selecting, and implementing information security protocols through a set of processes that can be integrated in an organization's SDLC. Relatedly, Microsoft declared conformance with ISO 27034-1 in May 2013.
6	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Major	Annex E	The scope of NIST SP 800-193 could easily apply to IoT and convey important priorities for Protection, Detection and Recovery. Currently the document does not list a reference to SP 800-193.	Add Special Publication 800-193 (DRAFT), Platform Firmware Resiliency Guidelines (hyperlink: https://csrc.nist.gov/publications/detail/sp/800-193/draft)
7	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Major	Full document	Lack of standards for managing devices at scale or recovery	There are no to very few mentions of the challenges to manage devices and their security at scale (such as provisioning for example). The addition of NIST 800-193 as a reference would help, but it doesn't address the necessity to control and manage IoT devices at scale.
8	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Minor	Line 1760, page 47	Additional clarity required for section on "Market Impact"	Replace current language with the following: "Market Impact? The AES standard has widespread market acceptance including testing and validation of thousands of implementations which would, as a result, have a strong accompanying market impact. In contrast, however, some of the recently approved RFID and lightweight cryptographic standards have no or few commercial implementations with a weaker market impact and may require adjustment and innovation for the IoT."

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

April 18, 2018

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

9	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Minor	Line 1783-91, page 48	Section on "Possible Standards Gap" includes information that should instead be included within section on "Market Impact"	Replace current language with the following: "Market Impact? Market implementations are lagging for cyber incident management for IoT systems. Some IoT systems are not able to use software patches to fix cybersecurity flaws. In such cases, cyber incident management is important for identifying incidents but remediation may require replacing IoT components. Replacement could be time consuming and expensive." "Possible Standards Gaps? Some IoT systems are not able to use software patches to fix cybersecurity flaws. An area for new standards development could be with respect to remediation (compensating controls) when software patches are not feasible."
10	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Minor	Line 1802-08, page 48-49	Section on "Possible Standards Gap" includes information that should instead be included within section on "Market Impact"	Replace current language with the following: "Market Impact? Detecting malware in software is technically challenging. This challenge would apply to firmware and drive additional cost considerations." "Possible Standards Gaps? Developing best practices for avoiding malware in firmware could be an area for new standards development."
11	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Minor	Line 1860-62, page 50	Further clarification required on "Market Impact" which appears to be more of a comment towards "Possible Standards Gap"	Replace current language with the following: "Market Impact? Unknown" "Possible Standards Gaps? Although standards exist, practical application to IoT systems has not been consistently demonstrated and is affecting implementation. Additionally, existing standards are not specific to IoT and should be reviewed to determine if they are sufficient or require revision for IoT systems."
12	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Minor	Line 1930, page 51	Section on "Market Impact" needs further development	Replace current language with the following: "Market Impact? Despite known impacts of insecure software, detecting malware in software is technically challenging and could be time consuming and expensive."

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

April 18, 2018

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

13	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Minor	Line 1962, page 52	Section on "Market Impact" needs further development	Replace current language with the following: "Market Impact? It is unclear if system security engineers apply systems engineering practices to IoT systems and any such services gap would require additional cost or implementation of new resources."
14	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Minor	Table 4, Line 1989, Page 53-54	Assuming Table 4 is intended as a summary for Annex D, TCG standards are listd in Annex D for "Cryptographic Techniques" and "Identity and Access Management", but are not listed in Annex D for "Security Automation & Continuous Monitoring" or "Software Assurance"	Add "TCG" in the column "Examples of Relevant SDOs" for rows "Cryptographic Techniques" and "Identity and Access Management" Remove "TCG" from the column "Examples of Relevant SDOs" for rows "Security Automation & Continuous Monitoring" and “Software Assurance”
15	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Minor	Line 2179, page 107	Section Annex D tables for IT System Security Evaluation should list IIC activities related to the IoT Security Maturity Model	Insert a new row mentioning IIC and pointing to the initial IIC SMM document published April 9. An accompanying practitioner's guide will be published around mid-year. At this point the document provides guidance and has not been approved as official standards.
16	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Minor	Annex D, "Identity and Access Management"	Missing standard in "Software Assurance" (Annex D) category that is "Under Development"	Add "Software Updates for Internet of Things (SUIT)" as standard in "Software Assurance" section (also see comment 13) - Information can be found at https://datatracker.ietf.org/wg/suit/about/
17	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Minor	Annex D, "Software Assurance"	Both SUIT and TEEP should be listed under "Software Insurance" instead of "Identity and Access Management"	While SUIT is about the firmware and TEEP about the "app" code inside the TEE chip, both are making sure that the software is the right software (for some definition of "software").

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

April 18, 2018

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

18	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Minor / Editorial	Line 1881-91, page 50	"Market Impact" appears to be more of a comment towards "Possible Standards Gap" and there are various grammar mistakes in the "Possible Standards Gap" section	Replace current language with the following: "Market Impact? Unknown" "Possible Standards Gaps? Many of these existing standards have widespread market acceptance with numerous commercial implementations. However, updates and/or new standards may be needed to deal with the IoT cybersecurity considerations listed at the beginning of Section 8. Additionally, many of these existing standards may require updates and/or new standards to address IoT networks that have the potential for spontaneous connection (due to the networking) without a system view. Such IoT systems cannot be planned or secured well using traditional approaches to security since system compositional or emergent properties would never be seen by a risk manager. IEEE 802.15.7 is a physical layer specification for visible light communication. Standards from the viewpoint of application service function development have yet to be developed."
19	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Editorial	Line 1705, page 46	Additional period and space at end of sentence	Remove additional period and space.
20	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Editorial	Line 1740, page 47	Inclusion of two unnecessary "-"s in the words "memory - and power - limited devices"	Remove both unnecessary "-"s and replace with "memory and power limited devices." Or alternatively include proper spacing between each "-".
21	Benedikt Abendroth, Microsoft, benedikt.abendroth@microsoft.com	Editorial	Line 1830-31, page 49	Inclusion of an unnecessary space in between lines and incorect capitalization.	Remove the unnecessary space in between lines and change the word "Provides" to "provides" since it is not the begining of a new sentence but the extension from the previous.