Microsoft's Feedback on the Draft Whitepaper on IoT Criteria for a Labeling Program from the National Institute of Standards and Technology

Microsoft Corporation ("Microsoft") welcomes the opportunity to provide comments to the National Institute of Standards and Technology ("NIST") in response to its August 2021 "Draft white paper with draft criteria for a labeling program on cybersecurity capabilities of Internet-of-Things (IoT) devices".[1]

We appreciated the detailed and thorough work that went into this draft as well as NIST's open and continued collaboration on all its standards and guidance documents. Microsoft reviewed this white paper with the intention providing clear, actionable recommendations. Microsoft strongly supports the goal of enhancing the security of IoT devices.

In the context of a consumer labeling program, Microsoft believes that a thoughtful, nuanced, and consistent approach to scoping the set of devices the criteria is applied to can assist manufacturers in prioritizing security capabilities and documentation resources towards the classes of devices presenting the greatest security and safety benefits for consumers.

In the table below, we have chosen to respond with direct references to the draft publication and recommendations:

Section	Comment
General (for the whole document)	Recommend using term "IoT product" versus "IoT device" consistently throughout the document. Ideally there is a formal definition for "IoT product" and it lists the physical device as an example in addition to the current examples of the "cloud backends, mobile applications and secure hubs".
Table 1 **Row: Asset Identification**	Term "product component host" first used in potential criteria #1 is not defined. Recommend adding a definition. (This term is used six times in the whitepaper.)
Table 1 **Row: Data Protection**	Microsoft strongly supports this criterion, especially as it relates to protecting the IoT component identity: "2. The ability to protect the product component's stored data from unauthorized change (e.g., protect against injected code or data manipulation attacks)". It may be helpful to highlight that stored information supporting device authentication is covered by the existing Data Protection criteria.

[1] https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/iot-device-criteria

Section	Comment
Table 1 **Row: Product Configuration**	Consider revising potential criteria #4 "4. The ability for authorized individuals and other IoT product components to restore the product component to the default secure configuration" in the following ways: a. Place the adjective "authorized" explicitly in front of both nouns (i.e., "other authorized IoT product components"). Other authorized IoT product components should be able to initiate restore, whereas unauthorized IoT product components should not be able to initiate restore. Justification: Some IoT product components may be less trusted and should not be authorized to reset other components. Note: There are eight instances of this text: "authorized individuals and other IoT product" in the document. b. Because the criterion only refers to the restoration of a single IoT product component, please consider if the criterion should be restated to restore an appropriate set of the IoT product components while not impacting IoT components shared between customers (e.g., a cloud back-end). For example, "restore all the non-shared product components". c. Append the sentence with "(inclusive of security updates)" to clarify the "default secure configuration" includes security updates.
Table 1 **Row: Data Protection**	Editorial: In potential criterion #1, recommend revising from "modules maybe dependent" to "modules may be dependent"
Table 1 **Row: Data Protection**	Criterion #4 uses the phrase "delete data at rest" which would require implementations to explicitly delete data (e.g., by overwriting it byte by byte). The phrasing in criterion #3 of "inaccessible to anyone, whether previously authorized or not" provides more flexibility to achieve the intended outcome (e.g., overwriting a cryptographic key used to encrypt data). Recommend revising #4 using the phrasing from #3.
Table 1 **Row: Data Protection**	In addition to the Potential Criteria in the draft that include protection for data at rest and in transit, we recommend the addition of the capability to protect data "in use." The addition of a capability to protect data in use would prevent an authorized person connecting to an IoT component over a network interface from being able to retrieve data currently in the runtime memory of the component. For devices with multiple users, protection for data in use could help protect each user's private information from each other.
Table 1 **Row: Software Update**	Editorial: There seems to be a word missing in the criterion #1. Recommend revising "through remote" to "through remote means" to match similar text in 8259A.
Table 1 **Row: Software Update**	Editorial: Recommend revising the note at the bottom of the potential criteria column from "components by be dependent" to "components may be dependent".

Section	Comment
Table 1 **Row: Cybersecurity State Awareness**	We recommend including the following Additional Criterion: "The ability to only use authorized software (i.e., use of an allowed list, software publisher signature check, etc. prevents unverified or unauthenticated software from being used)" Justification: Requirements to verify and authenticate software when updates occur are important; however, other threats exist that can compromise the integrity of software. If the IoT product component does not use unauthorized software it can reduce the potential for compromise.
Table 1 **Row: Cybersecurity State Awareness**	We recommend inserting an additional example for criterion #1 in the parenthesis: "installation of unauthenticated updates".
Table 1 **Row: Cybersecurity State Awareness**	Potential Criterion #3, states "The ability to prevent any unauthorized edits of state information by any entity" (a) Please clarify if "state information" refers to one or more of "cybersecurity state information (e.g., log entries)", information protected by a root of trust for measurement and reporting (e.g., a Trusted Platform Module), or general device state information (e.g., runtime state). Microsoft supports protection of all three examples. (b) If "state information" refers to the protection of "cybersecurity state information" of data at rest, consider if this criterion should be moved to the "Data Protection Row.
Table 1 and Table 3 **Row: Product Security**	Recommend revising current text in the left column from: "Product Security: The IoT product can perform other features and functions across some or all of its components to make IoT products minimally securable for the sector." to "Product Resilience: IoT product can perform some functions across some or all of its components to make the IoT product minimally usable when connectivity is disrupted" because it aligns more closely with the stated criteria.

Section	Comment
Table 2	These three criteria refer to the time when a product will receive security updates: The Row "Documentation" includes Potential Criterion #1h, "Expected lifespan, anticipated cybersecurity costs related to the IoT product (e.g., price of maintenance), and term of support" Row Education and Awareness includes Potential Criterion #1d, "How to maintain the IoT product and its product components during its lifetime, including after the period of security support (software updates and patches) from the manufacturer." Row Education and Awareness includes Potential Criterion #4, "The product packaging provides information consumers can use to make informed purchasing decisions about the security of the IoT product (e.g., the duration and scope of product support via software upgrades and patches)." We recommend allowing flexibility for the manufacturer to specify a minimum period of support with the opportunity to extend the support window (e.g., depending on the popularity of the product, etc.).
Table 2 **Row: Documentation**	Potential Criteria #2 states, "2. Document what other IoT components other than the IoT device (e.g., cloud backend, mobile app, secure hub) are necessary to using the IoT product's functionality beyond basic operational features (e.g., an unconnected smart lightbulb may still illuminate in one color, but its smart features cannot be used with other product components unless they are connected)." Recommend inserting "security update source" in the first parenthesis list as an example to encourage manufacturers to clarify the source of updates.

Section	Comment
Table 2 **Row: Documentation**	Potential Criteria #5a states, "Document product design and support considerations related to the IoT product, such as: a. All hardware and software components, from all sources (e.g., open source, propriety third-party, internally developed) used to create the IoT product (i.e., used to create each product component)" with a footnote clarifying, "While this information would be provided by a Software Bill of Materials (SBOM), what is being discussed here is significantly less elaborate than what is normally meant by an SBOM. More details on SBOM can be found at https://www.ntia.gov/SBOM" As written, this requirement is too expansive to be practical, especially when the IoT product component scope includes a cloud backend or an application running on a smart phone. Presumably it would need to include all hardware used to implement a cloud backend, tools used to develop and compile source code for components, operating systems, etc. Mandatory documentation needs to enable an authorized individual to determine the most recent security update available for the IoT product and verify it has been deployed.
Table 2 **Row: Documentation**	Potential Criteria #5c states, "Document product design and support considerations related to the IoT product, such as: c. Protection of software and hardware elements used to create the IoT product and its product components (e.g., secure boot, hardware root of trust, and secure enclave)" Does including this criterion in Table 2 mean the IoT product passes if the documentation exists, even if the documentation states "no protection"? Recommend moving the criteria to a technical capability to encourage adoption of security technologies (e.g., secure boot, roots of trust, address space layout randomization, etc.).
Table 2 **Row: Documentation**	Potential Criteria #5d states, "Document product design and support considerations related to the IoT product, such as: d. Consideration of the known risks related to the IoT product and known potential misuses" It seems counterproductive to publicly document potential ways to misuse a product as that would likely facilitate others to misuse it too. Recommend clarifying the expectation is such documentation and mitigation information remains in the manufacturer's records and need not be disclosed.

Section	Comment
Table 2 **Row: Documentation**	Potential Criteria #5e states, "Document product design and support considerations related to the IoT product, such as: e. Expected data inputs and outputs (including error codes, frequency, type/form, range of acceptable values, etc.)" The level of detail required is unclear. Is this criterion intended to be a high-level troubleshooting guide for users or a detailed document for a developer to integrate with individual IoT components? Recommend the former for a consumer audience. If it is the latter, recommend clarifying the expectation is such documentation remains in the manufacturer's records and need not be disclosed.
Table 2 **Row: Documentation**	Potential Criteria #5g states, "Document product design and support considerations related to the IoT product, such as: g. Laws and regulations with which the IoT product and related support activities comply" Companies generally produce products with the intent of complying with all local laws and regulations. Laws and regulations can be ambiguous and dynamic, sometimes requiring product updates to remain compliant with changes. Recommend restating this criteria as, "g. Countries and regions where the product is available" A example of is located here: Microsoft 365 and Office 365 International Availability.
Table 2 **Row: Documentation**	Potential Criteria #7c states, "7. Document the secure system lifecycle policies and processes associated with the IoT product, including: c. Any post end-of-support considerations, such as in the event that a vulnerability is discovered which would significantly impact the security, privacy, or safety of customers who continue to use the IoT product and its product components." An example would be helpful. Is an example "a manufacturer documenting they will provide post end-of-support security updates for a fee for an additional time period?" If so, we recommend reconciling with Table 1, Row Documentation, Criterion 1h ("1h. Expected lifespan, anticipated cybersecurity costs related to the IoT product (e.g., price of maintenance), and term of support")?
Table 2 **Row: Information and Query Reception**	Editorial: In Possible Criterion #2, replace "repair technical" with "repair technician".

Section	Comment
Table 2 **Row: Information Dissemination**	Potential Criteria #2 states, "2. The procedures to support the ability for the manufacturer and/or supporting entity to alert appropriate ecosystem entities (e.g., common vulnerability tracking authorities, accreditors and certifiers, third-party support and maintenance organizations) about cybersecurity relevant information such as:" The paragraph itself (ignoring the list below it) could be read as suggesting manufacturers have (somewhat unclear) reporting obligations to ecosystem entities. Recommend the paragraph is revised to reference best practices such as ISO/IEC 29147:2018 on Vulnerability Disclosure[2] or The CERT Guide to Coordinated Vulnerability Disclosure.[3] For each of the items in the list below the paragraph (items "a" through "f"), recommend clarifying if these are intended to be distributed as public information or shared confidentially. If intended to be shared confidentially, recommend clarifying the criteria manufacturers should use to determine who the information needs to be shared with.
Table 2 **Row: Information Dissemination**	Potential Criteria #2f states, "2. The procedures to support the ability for the manufacturer and/or supporting entity to alert appropriate ecosystem entities (e.g., common vulnerability tracking authorities, accreditors and certifiers, third-party support and maintenance organizations) about cybersecurity relevant information such as: f. A risk assessment report or summary for the manufacturer's business environment risk posture" Ideally criterion "f" references public content public companies are already submitting to regulators. (E.g., consider adding the United States Securities and Exchange Commission Form 10-K as an example, if applicable.)

[2] https://www.iso.org/standard/72311.html

[3] https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

Section	Comment
Table 2 **Row: Information Dissemination**	Potential Criteria #3a states, "3. The procedures to support the ability for the manufacturer and/or supporting entity to notify customers of cybersecurity-related events and information related to an IoT product throughout the support lifecycle, such as: a. New IoT device vulnerabilities, associated details, and mitigation actions" (a) Consider replacing "IoT device" with "IoT product". (b) Please consider the FAQ located here https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-28460 as an example best practice.
Table 3	Additional Criteria Recommended: Proposed IoT Product Cybersecurity Capability: "Minimal maintenance for connected devices" as an optional criterion. Proposed Criteria: 1. The default ability for the manufacturer to automatically install software updates to all components throughout the product's supported lifecycle. 2. The persistent ability (by default) for the manufacturer to detect if the product enters a degraded cybersecurity state and to automatically apply software and configuration updates to IoT product components to restore the device to a trusted cybersecurity state (inclusive of updates). The criteria would assist consumers in identifying products that remain secure over the product lifecycle with minimal consumer action.
Table 3	Additional Criteria Recommended: Because IoT component identity is the basis for addressing so many security related scenarios (especially over a network), Microsoft strongly recommends NIST consider additional criteria for Table 3 that IoT components are able to identify themselves using a strong cryptographic identifier (e.g., able to be used for component authentication and logging). It is preferable that cryptographic identifiers for IoT components be provisioned by the manufacturer, but it is also adequate if cryptographic identifiers are generated during the process of putting a device into service or can be regenerated to preserve privacy.

Section	Comment
Table 3 **Row: Asset Identification**	Recommend revising current text in the left column from: **"Asset Identification:** The IoT product can uniquely identify and inventory all of the IoT product's elements/components." to **"Asset Identification:** The IoT product can uniquely identify and inventory all of the IoT product's components." because "product element" is not defined.
Table 3 **Row: Asset Identification**	Potential Additional Criterion #2 says: "2. The ability to create an inventory of information about other product components, including but not limited to identifiers." (a) Consider including "version information" as an example in addition to identifiers. However, "version information" may be restricted to authorized users or other authorized IoT components. (b) Ideally this information is easily available to the consumer so they can check their patch status (if manual patching is required).
Table 3 **Row: Product Configuration**	Proposed Additional Criterion #4 says, "4. The ability for authorized individuals and other IoT product components to restore the device to the default secure configuration." Consider if "device" should be replaced with "IoT product".
Table 3 **Row:** Logical Access to Interfaces	Microsoft strongly supports this additional criterion: "1c: The ability to participate in a secure authentication mechanism with other product components (e.g., help gather authenticators, assert authorization based on authentication)."