Report on CTA Pilot of the NIST Consumer IoT Cybersecurity Label Proceeding

Version 1.0
March 15 2022

CONTENTS

CTA Pilot – NIST Consumer IoT Cybersecurity Label Proceeding

1 EXECUTIVE SUMMARY

This Pilot was conducted in the context of the Department of Commerce National Institute of Standards and Technology (NIST) program, *Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software*.[1]

The NIST program was responsive to Executive Order 14028, which required the Department of Commerce, acting through NIST, to *"initiate pilot programs informed by existing consumer product labeling programs to educate the public on the security capabilities of internet-of-Things (IoT) devices and software development practices, and shall consider ways to incentivize manufacturers and developers to participate in these programs."*

The Pilot tested the February 2022 NIST recommendations for labeling programs for consumer IoT cybersecurity ("NIST Criteria", [6]). The NIST Criteria were developed in a broad multi-stakeholder process involving subject matter experts from NIST, industry, academia and more. However, it had not previously been tested, either on paper or in practice.

The Pilot compared the recommended elements listed in the Criteria vs. representative industry programs and standards ("Schemes") for IoT cybersecurity. Data are recorded in spreadsheets taken from the NIST On Line Informative Reference program[2], where the NIST Criteria are the "focal document" and the industry documents are the "reference documents".

<u>Technical Recommendations</u> in the NIST Criteria were compared to

1. UL *MCV 1376* [14]for an example of the security framework used by a 3rd-party conformity assessment program, and
2. (Draft) CTA-2088-A, *Baseline Cybersecurity Standard for Devices and Device Systems* [2] for the basis of a hypothetical "self-declaration of conformity" program (SDOC).

<u>Non-Technical Recommendations</u> of the NIST Criteria were compared to

3. UL MCV 1376 [14]and the UL *IoT Security Rating* program [13]for 3rd-party programs, and
4. *The BSA Framework for Secure Software v1.1* [4] from BSA | The Software Alliance for SDOC programs.

<u>Conformity Assessment Recommendations</u> of the NIST Criteria were compared to

5. The UL *IoT Security Rating* Program [13]

[1] NIST web site *Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software*, https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/cybersecurity-labeling-consumers-internet-things

[2] See https://csrc.nist.gov/Projects/olir for more information on the NIST On Line Informative Reference program.

Label Recommendations

6. The UL *IoT Security Rating Program* [13] and
7. UL MCV 1376 [14]

This Pilot deviated from the NIST Criteria in one important way. The NIST Criteria assumes a “gestalt” product model (see section 2.4). This Pilot assumes a basic hardware device and did not attempt to test the Criteria against other product components such as apps or cloud services.

While the body of work resulting from NIST’s efforts was rigorously reviewed by many, initial testing of a product will always identify potential improvements. This is the purpose of pilot testing in industry, and the purpose of this Pilot as well. We therefore respectfully include recommendations for consideration by NIST regarding potential improvements to the Criteria in Section 8 of this report.

Summary of Findings:

Results are detailed in Section 4, *Findings and Recommendations*. A short summary is below.

- The “gestalt” product model combines the device and embedded software with cloud services and apps; some profiling or new Criteria should be considered instead.
- The combination of Documentation requirements and Information Dissemination requirements raised concerns; the Documentation list is extremely broad and goes beyond what should be needed at the Information Dissemination stage (i.e., the incident mitigation stage).
- Documentation to be disseminated should be directly applicable to cybersecurity purposes, such as mitigating vulnerabilities or breaches.
- The OLIR Template has no apparent way to link the multiple components of an IoT product (device and associated software, apps, cloud services) as a gestalt.
- Risk assessment options should be added to Data Protection and vulnerability disclosure.
- Each product component is required to sanitize data when transmitting to other components; it is not always possible for a component’s software to know the input requirements of the other components.
- Software Bill of Materials is a promising technology but not ready as a baseline requirement yet.
- The NIST Criteria should not discuss or require commercial terms such as support life.
- Further informative text on the risk of asset identifiers and PII would be helpful to users of the NIST Criteria.

Although NIST staff was briefed on the effort, there was no direct involvement of NIST staff in this test of the NIST Criteria.

2 PILOT OVERVIEW

In February 2022, NIST offered the opportunity to contribute pilots of their *"Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products"* ("NIST Criteria", [6]). Information on this pilot contribution program is presented at the web page, *Consumer Cybersecurity Labeling Pilots: The Approach and Contributions*[3] ("Request for Contributions").

In the context of the Request for Contributions, this industry partnership IoT device pilot (the "Pilot") tests the NIST Criteria against industry Schemes for two conformity models: 3rd-party conformity assessment, and self-attestation of conformity. UL's IoT Security Rating program and the underlying *UL MCV 1376* security framework was used as the Scheme for the 3rd-party program; CTA and BSA documents were paired to create a realistic Scheme for self-attestation.

2.1 Pilot Partners

The Pilot was hosted by CTA. Industry partners contributed important experience and technical expertise. A general overview of the partner organizations can be found in About the Partners. Specific roles are identified here.

- Consumer Technology Association (CTA)

  CTA hosted this effort and contributed member expertise in IoT device cybersecurity. The standards development arm of CTA contributed (Draft) CTA-2088-A [2], a technical standard on hardware device security. Much of the NIST Technical Criteria map to the standard.

- UL Inc.

  UL Inc. is an international conformity assessment body. UL contributed expertise in all aspects of IoT device security: technical criteria, conformity assessment, labeling and informing consumers. UL's MCV 1376 security framework [14] and their associated IoT Security Rating Program [13] map to most of the full NIST Criteria and related requirements.

- SpireSpark International Ltd.

[3] https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/consumer-cybersecurity-labeling-pilots-approach

SpireSpark is a consulting firm specializing in the development of conformity assessment programs and has done extensive research on IoT security standards in the UK, EU and US. SpireSpark contributed technical and operations expertise for this Pilot.

2.2 Pilot Goals

The goal of this Pilot is *to test the NIST Consumer IoT Cybersecurity Label program documents against existing industry programs and technical documents, in as complete a fashion as possible.*

According to the NIST Request for Contributions program website[4], the Request for Contributions program involves contributions from stakeholders, "*regarding current or potential future labeling efforts for consumer IoT products and consumer software, and how those efforts align with the NIST recommendations."*

Perfect alignment between industry programs and the NIST Criteria was not expected, and this was confirmed during this Pilot. Where gaps or differences were found, they are documented in this report along with recommendations for improving the alignment.

It should be noted that there are relatively few occurrences of misalignments. It is likely this low rate of misalignment is due to an aggressive and successful public-private stakeholder process led by NIST to develop the Criteria.

2.3 Pilot Structure and Methodology

The NIST OLIR template for technical and non-technical criteria was used as a framework for studying and comparing the elements of the NIST Criteria and industry programs. Matches were identified, entered, and categorized as required in the OLIR submission guidance document NISTIR 8278A [12].

Outside the review of the NIST Criteria based on the OLIR template, there are some additional considerations on Labeling (see Section 5).

2.4 The Pilot and the NIST Criteria "Gestalt" Product Model

NIST has a gestalt or holistic product model for cybersecurity. As explained in the NIST Criteria [6],

> **In the context of these labeling recommendations, an IoT product is defined as an IoT device and any additional product components that are necessary to use the IoT device beyond basic operational features.**

[4] https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/consumer-cybersecurity-labeling-pilots-approach

As an example, a video doorbell might include

- The hardware component (video doorbell itself),
- a smartphone app that can control the hardware and display front-door video, and
- a cloud video storage service that is available to owners of the device.

This example is used to illustrate the complexity of the IoT eco-system. It encompasses clear sets of components that together provide a segmented and inter-dependent environment.

Assessment of the IoT eco-system is divided into 4 focus-areas:

- ***IoT Devices:*** Refers to the functional testing and evaluation of the physical IOT Device, the embedded software for compliance and certification requirements, and general security assurance. Example standards include CTA-2088, EN 303-645, and NIST 8259A.
- ***Governance:*** Refers to formal processes for managing towards security-based outcomes. Governance is applicable to various stakeholders in terms of principles, norms, rules, decision-making, procedures, programs, and non-functionality of devices within the IoT Eco-system while not limiting governance to the application of data integrity and data security of IoT devices, thereby defining security postures of organizations. Examples include CMMC, CMMI, and GDPR.
- ***Supporting Software and Applications:*** Refers to ancillary services supporting non-device functionality of the IoT product, including web applications, computer-based application and mobile applications. The security performance of such supporting software and applications affects the overall security of the environment, and as such may require targeted scopes. Examples include Mobile Application and Web testing according to OWASP Standards.
- ***Cloud Based Services*****:** Infrastructure and cloud-based environments provide data management and other capabilities. They also play a role in IoT Security. Important here are best practice principles for providing security assurance within cloud computing. The Cloud Security Alliance STAR attestation is an example.

While all four areas are important to keep in mind during the design, development, and product lifecycle of an IoT device, it is necessary to delineate between these areas when defining Device focused IoT Security Criteria.

Under the NIST Criteria gestalt product model, the full “product” in the example above is the device, smartphone app, cloud video service, as well as any number of governance activities. This means the NIST Criteria technical and non-technical recommendations, under this gestalt model, would be applied to the smartphone app and cloud services, along with the hardware component.

The NIST Criteria are based on fundamental cybersecurity principles, but in practice this extended model creates challenges for the product maker. For example,

- The cloud services may be under a trustmark, such as the CSA STAR program, that does not follow the hardware-centric NIST Criteria.

- A device may not be sold with a smartphone app, but such an app may be required to use "the full features" of the product, such as a wearable that leverages existing exercise apps. The product maker may have no relationship to the various app developers in the ecosystem.
- Examples in the NIST Criteria are hardware-focused, e.g., "secure boot" or "authorized repair centers"; there is no clear off-hardware element.

The Schemes in this Pilot do not consider cloud services or smartphone apps. More specifically, using the four divisions of the IoT ecosystem as described above, the Schemes in this Pilot only consider 'IoT Devices' as in scope.

3 SCHEME OVERVIEWS

3.1 3rd Party Assessment Scheme – UL MCV 1376 / UL IoT Security Rating Program

The IoT Security Rating [13] program offers a tiered, light-weight product security verification solution, which is driven by 'baseline' security practices, and results in a differentiated product security label. The solution features 5 security levels, ranging from simple, absolute minimum security practices to more comprehensive security implementations. As a result, the evaluated product is awarded the achieved security level (Bronze, Silver, Gold, Platinum, or Diamond), which is displayed through the UL Verified Mark. This Mark can be placed on the product, product packaging, or within a retail environment (physical store or webshop).

IoT Devices aiming to achieve the UL Verified Mark for any of the five security levels are evaluated by using the security framework defined in *UL MCV 1376 [14].*

UL MCV 1376 [14] is a baseline-driven security verification framework that groups sets of industry-referenced security best practices into 5 different tiers ("levels") based on their necessity for implementation. Level 1 references best practices that are considered an absolute minimum (a "baseline") for any connected device, followed by 4 more levels of increasingly expanding sets of industry-acknowledged security capabilities that become more advanced and comprehensive in nature. UL MCV 1376 references and/or maps to various industry-leading security frameworks, such as EN 303 645 [5] and NIST IR 8259A [9].

Technical Recommendations in the NIST Criteria were compared to the UL *IoT Security Rating* [13] and the underlying security framework, *UL MCV 1376* [14], to test the NIST Criteria against an industry 3rd-party conformity assessment program.

3.2 Self-Declaration of Conformity Scheme – CTA-2088-A and BSA Framework

This portion of the Pilot assumes a hypothetical self-declaration of conformity (SDOC) Scheme. The Scheme is 'hypothetical' because there is no current framework under which this Scheme would be applied; establishing such a framework is a subject of discussion in industry at this time.

Under this Scheme, two sets of industry documents were combined to cover the NIST Criteria's technical and non-technical recommendations. Together the two documents cover the majority of the NIST Criteria.

Draft CTA-2088-A

The Technical Recommendations in the NIST Criteria were compared to the pre-publication draft of CTA-2088-A, *Baseline Cybersecurity Standard for Devices and Device Systems* [2]. ANSI is the American National Standards Institute, the organization that oversees the development of American National Standards (ANS). CTA is an ANSI-accredited standards development organization.

CTA-2088-A is a revision of ANSI/CTA-2088 [1]; it was revised in part to take into account the evolution of the NIST Baseline and NIST Criteria. The earlier document is an American National Standard (ANS) published in December 2020. However, the responsible CTA working group made selected modifications to 1) improve conformance testability, and 2) align to the NIST Criteria as it evolved.

The CTA-2088 family of standards derives from the Council to Secure the Digital Economy's C2 Consensus, which is a sector-specific IoT cybersecurity baseline that maps to earlier NIST work, the NISTIR 8259A baseline [9].

Draft CTA-2088-A is in the process of being published. It is expected to be available in May 2022 and a pre-publication version was used for this Pilot. CTA-2088-A is expected to complete the necessary process to become an ANS and will be available as "ANSI/CTA-2088-A" in August 2022 or soon after. ANSI/CTA-2088 and CTA-2088-A (when published) are available as no-cost downloads at https://shop.cta.tech/collections/standards/cybersecurity.

The BSA Framework

The Non-Technical Recommendations of the NIST Criteria were compared to *The BSA Framework for Secure Software v1.1* [4], publicly available from BSA | The Software Alliance.

4 FINDINGS AND RECOMMENDATIONS

This section identifies differences between industry documents and the NIST Criteria.

> **It is important to note that the NIST Criteria are being tested in this Pilot. Because this is a test of the elements of the Criteria, each option or optional element is examined as if *required*, for purposes of the test.**

The NIST Criteria are not being applied in this Pilot; they are being tested against the Pilot documents in the two Schemes. Therefore, it is appropriate to treat each item and example *as a requirement for purposes of the test*. However, this testing does – as one might expect – uncover areas of potential improvement for the NIST Criteria.

> **It is important to note that despite the use of "such as" or "for example" language in the NIST Criteria, it still may not be possible to exclude unnecessary, inapplicable or unfeasible line-items from a regulatory structure, should such a structure be established based on the NIST Criteria. Therefore, the NIST Criteria are judged here as if each example item is strictly required in a non-voluntary process.**

4.1 Review the Gestalt Product Model as Applied to Ancillary Services

Summary: The gestalt model applies the NIST Criteria to the IoT device, plus any apps or cloud services required for the full functionality of the IoT product. Profiles or variations on the NIST Criteria would be better suited to such "ancillary services".

The Schemes in this Pilot do not consider cloud services or smartphone apps or other non-device capabilities shipped with the IoT device. There are resources for verifying the cybersecurity of such ancillary services.

The Cloud Security Alliance (CSA, https://cloudsecurityalliance.org/) has excellent resources for cloud-based services. A profile of the NIST Criteria or a new Criteria that focuses on cloud requirements would be appropriate. For example, the CSA STAR program has a trustmark which can be displayed on a website. The program has elements that are cloud-specific but not appropriate for devices, such as audit requirements.

Similarly, the Open Web Application Security Project® (OWASP, https://owasp.org/) has excellent resources, such as the Application Security Verification Standard (ASVS) Project (for web apps) and the Mobile Security Testing Guide (for mobile apps).

However, retesting against ancillary services like cloud and apps may show more systemic issues with the current NIST Criteria. More specific versions or profiles of the NIST Criteria would be appropriate for categories outside IoT devices as defined above.

> **Recommendation**: Consider profiles or distinct forks of the NIST Criteria for non-hardware product components rather than current gestalt product model for future iterations of this program.

4.2 Review and Reduce Documentation Requirements

Summary: The Documentation section should be scaled back to cybersecurity-specific elements that would have a clear purpose in mitigation of a cybersecurity incident. Several such items are identified in this section.

> **It is important to note that the analysis in this section is based on the assumption that Criteria Information Dissemination-2a implies a potential release of unnecessary or otherwise-confidential information. Therefore, the Criteria are judged here as if each item is *required* to be released under applicable circumstances (e.g., incident mitigation).**

The requirements in the Criteria section on “Documentation” are extensive. Most are items collected anyway during the development of product requirements. However, not all of these items serve a direct purpose in enhancing the cybersecurity of the IoT product. Some are more likely to be useful or necessary in normal business operations during the product development phase. See the following from the Information Dissemination section:

> Information Dissemination-2a Applicable documentation captured during the design and development of the IoT product and its product components.

Therefore, each required Documentation element should be carefully screened for whether having it in the Documentation group—for presumed later disclosure—*directly and materially contributes to the actual cybersecurity of the IoT product and its release would contribute to mitigation in the event of an incident*.

As an example, in a normal product development lifecycle, an early phase will involve documenting things like expected customers and use cases, how the product is expected to be used, market requirements, estimated cost of manufacturing, and so on. This information is used to justify moving to the next stage, product development.

The organization will collect some of the same information for cybersecurity purposes, as the organization performs threat modeling and risk analysis.

The threat modeling and risk analysis directly supports cybersecurity goals. The further information collected during the product planning stage may overlap information collected for cybersecurity goals but isn’t necessarily required.

As the SDOC Scheme mapping shows, the NIST Criteria “Documentation” requirements are mostly covered by BSA [4] TV.1, which requires threat analysis. The process of doing threat analysis will involve collecting most of the elements of Documentation-1a. That is, threat analysis begins with assessing scope and risk (see, e.g., [3]). Elements of threat analysis include "*expected customers and use cases*" (Documentation-1a(i)), "*physical use*" (Documentation-1a(ii)), "*network access and requirements*" (Documentation-1a(iii)), and so on.

When compared to UL [14], the NIST Criteria "Documentation" requirements are also much more intensive, with only one of the NIST sub-criteria directly mapping to the UL security framework, specifically Documentation-1f. This gap is mostly due to the intended use of the UL IoT Security Rating program and the security framework described in UL [14], which, while aligned with industry best practices for formal accreditations and approvals, is itself intended to be used in the capacity of achieving a Marketing Claim Validation, lending the focus to be on the adherence to technical security best practices for the device and less so on the documentation involved in the product's development and further lifecycle.

4.2.1 Documentation Requirements – Customers, Use Cases, Laws and Regulations

BSA [4] TV.1 does not cover the "expected customers and use cases" requirement in Documentation-1a(i). The requirement to collect such information is as follows.

> Documentation-1a(i) Expected customers and use cases.

BSA [4] TV.1 also does not cover the "laws and regulations" requirement in Documentation-1a(vii). The requirement to collect such information is as follows.

> Documentation-1a(vii) Any laws and regulations with which the IoT product and related support activities comply.

Collecting this information may be helpful from a marketing perspective and from a more general product requirements planning perspective. However, the cybersecurity purpose of this specific information isn't entirely clear. A threat is valid regardless of who purchases the product, and a vulnerability may exist whether it is permitted or not by applicable law or regulation.

To the extent these data inform threat modeling, this information is typically collected in process flow diagramming in threat modelling.

> **Recommendation:** Remove Documentation-1a(i).
>
> **Recommendation:** Review Documentation-1a(vii); possibly focusing on 'requirements', for example, "*Additional requirements from* any laws and regulations…" Besides aligning this item with the other elements of Documentation-1a, if this change is made the -1a(vii) item will be supplementing the requirements extracted in the threat analysis phase required by TV.1.

4.2.2 Documentation Requirements – Lifespan and Anticipated Cybersecurity Costs

BSA [4] TV.1 also does not cover Documentation-1a(viii), *“Expected lifespan and anticipated cybersecurity costs related to the IoT product (e.g., price of maintenance), and length and terms of support.”*

This item is reasonable for internal business process documentation. It does not directly apply to cybersecurity of the product. Later NIST Criteria (“Information Dissemination-2(a)”) requires that the product developer have the capability to disseminate such information (“applicable documentation captured during design and development”); such internal information should not be required to be disclosed.

Recommendation: Remove Documentation-1a(viii).

4.2.3 Documentation Requirements – Documenting Product Components

The Documentation-1b item refers to listing, “All IoT components, including but not limited to the IoT device, that are part of the IoT product.” While threat analysis required by BSA [4] TV.1 would reasonably require documenting such components, the Schemes in this Pilot do not extend to cloud or app components.

Similarly, other line-items in the OLIR spreadsheet for this Scheme indicate that the response is provided for the hardware component only.

Recommendation: Remove the reference to “all…components” in Documentation and focus it on the specific component under review.

4.3 The OLIR Template Should Be Able to Handle All Product Components

Summary: The OLIR Template should be made hierarchical to include all product components of the IoT device or made explicitly flat for single components.

The current version of the OLIR Template [11] does not adapt well to the “gestalt IoT product component model” (see *Criteria IoT Product Model* in Section 2.4). The OLIR Template is suitable for a single component, such as a hardware product or a smartphone app. However, the Criteria refer to requirements that cross these boundaries. For example,

> Data Protection-1 Each IoT product component protects data it stores via secure means, including the ability to delete or render inaccessible data stored that is either collected from or about the customer, home, family, etc.
>
> Interface Access Control-2b Prevent unauthorized transmissions or access to other product components.

In these two examples, the language implies that the Template covers all the device’s product components. However, the non-hierarchical nature of the template means all components – device, smartphone app, web app, cloud services, etc. — must be covered in the one spreadsheet at a flat level. This is not impossible; a single instance of a Criteria could be replicated on multiple lines, with each component treated in one such line. But there is no field to identify the component type, so that will have to go in the Comments, or be built into the Reference Document element name.

Furthermore, the OLIR structure is designed for a single Reference document. Multiple Reference documents will make up any reasonable Scheme that is able to span hardware, cloud services, apps and other ancillary services.

> **Recommendation**: If the gestalt product model is retained, review the structure of the OLIR template such that a product hierarchy can be supported in entering data from a multiple-component product and with multiple Reference documents.

4.4 Review and Reduce the Data Protection and Risk Assessment

Summary: The Data Protection requirement for all external communications is too broad and should be modified with the option of risk assessment for appropriate use cases.

> Data Protection-2 When data is sent between IoT product components or outside the product, protections are used for the data transmission.

There are use cases where the data is considered "public" and not requiring of encryption. For example, drone footage returning wirelessly to a base station may be considered "open" and sent in the clear (note that this is a separate use case from the command & control link, which would require protection). This requirement should be updated to include "risk assessment".

> **Recommendation**: Add risk assessment to the Data Protection requirement, such that data worth protecting (based on risk assessment) is required to be protected.

4.5 Review the Requirement For Sanitizing Data Sent to Other Components

Summary: The Interface Access Control-2a requirement for data sent to other product components is less secure than if each component had responsibility for validating its own input, rather than for outputs to other components.

> Interface Access Control-2a Validate that data sent to other product components matches specified definitions of format and content.

Self-validation of a component’s inputs is a best practice. Validation of data transiting into the device aids security by stopping the subversion of the system by attackers. When subversive data is eliminated at the entry point it cannot be passed on to other product components.

Validation of *other* components' inputs is a good practice where possible. However, during the design phase, the developer of a product component may not know which other components the subject component will be matched up with, either pre-market or post-market. For example, a product component first shipped in Year X may be repackaged in Year X+2 with a new set of components. Or a product component may rely entirely on 3rd-party apps or services. Product component data requirements may change over time, making it difficult to keep each individual component in sync with the data sanitization requirements of the others. Conformity assessment is similarly difficult; the tester has all the burdens listed above.

A recommendation for the component to carefully format data before it goes to another component is a prudent best practice to ensure interoperability. For a security requirement that will be subject to conformity assessment, the device should be responsible for sanitizing its inputs.

> **Recommendation**: Revise the data sanitation requirement to make it specific to product components sanitizing their own inputs.

4.6 Review the Role of Software Bill of Materials (SBOM)

Summary: Hardware bill of materials is well-known. Software bill of materials is evolving and the wording of Documentation-1d should be reconsidered as to a SBOM requirement.

> Documentation-1d Product design and support considerations related to the IoT product, for example:
>
> i. 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).
>
> …

This item would seem to imply a requirement in the Scheme for SBOM documentation. While SBOM shows promise in NTIA- and CISA-led efforts and in proof-of-concept exercises, wide-scale piloting would be appropriate before including as a baseline requirement.

> **Recommendation**: Soften the requirement for SBOM while industry-wide piloting continues.

4.7 Remove Requirements On Commercial Terms

Summary: The NIST Criteria should not require actions that set or change commercial terms such as warranty or support terms.

> Information Dissemination-1a Updated terms of support (e.g., frequency of updates and mechanism(s) of application) and notice of availability and/or application of software updates.

Terms of support are a commercial issue. As written, this item does not directly address cybersecurity. In consumer products, updates are typically provided when the security team identifies and remediates a vulnerability, not according to a support agreement.

"Notice of availability and/or application of software updates" is a separate issue and should be treated in a separate item.

A second example is,

> Product Education and Awareness-1e Additional information customers 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).

As noted above, “duration and scope of product support” is a warranty topic.

> **Recommendation**: The NIST Criteria should not require actions that set or change commercial terms such as warranty or support terms.

4.8 Allow For Risk Assessment When Requiring Vulnerabilities to be Disclosed

Summary: The Information Dissemination-1d requirement, as written, does not take into account a risk-based prioritization of vulnerabilities and any decision process for disclosure.

> Information Dissemination-1d New IoT device vulnerabilities, associated details, and mitigation actions needed from the customer.

As NIST indicates in *Recommendations for Federal Vulnerability Disclosure Guidelines* @517, “For each vulnerability identified in government systems, the VDPO (Vulnerability Disclosure Public Office) in whose system the vulnerability exists must determine whether or not public disclosure is warranted.” While the situation is different, the criteria stated include points that should be considered in private industry for consumer technology, such as:

> *522 • The specific vulnerability is not publicly known (i.e., does not have a CVE number);*
>
> and
>
> *529 • The public is at risk of harm in some way or needs to take some action to secure themselves (e.g., install a patch, update software, or change their passwords).*

These are important elements of a vulnerability disclosure process that includes a decision whether to disclose publicly.

Recommendation: The NIST Criteria should take the risk assessment decision process into account.

4.9 Review Language on Information Dissemination List

Summary: As noted above, all information dissemination examples are treated in this Pilot as 'required'. Documentation to be disseminated should be directly applicable to cybersecurity purposes, such as mitigating vulnerabilities or breaches.

Information Dissemination-2 The IoT product developer can distribute information relevant to cybersecurity of the IoT product and its product components to alert appropriate ecosystem entities (e.g., common vulnerability tracking authorities, accreditors and certifiers, third-party support and maintenance organizations) about cybersecurity relevant information, for example:

a. Applicable documentation captured during the design and development of the IoT product and its product components.
b. Cybersecurity and vulnerability alerts and information about resolution of any vulnerability.
c. An overview of the information security practices and safeguards used by the IoT product developer.
d. Accreditation, certification, and/or evaluation results for the IoT product developer's cybersecurity-related practices.
e. A risk assessment report or summary for the IoT product developer's business environment risk posture.

- Item (a) in this list appears to refer to the Documentation section, which is overly broad. The term "applicable" is subject to interpretation and should be clarified; possibly by scoping the applicability of the information to the cybersecurity purposes.
- Item (b) is appropriate to the purpose of cybersecurity.
- Items (c), (d), and (e) do not appear to serve a cybersecurity purpose when disseminated.

Recommendation: Remove items (c), (d), and (e); also address the breadth of the Documentation section as described in item 8.4 above.

4.10 Include Cautionary Language Regarding PII for Asset Identification

Summary: The requirement for Asset Identification triggers privacy concerns despite limitations in the text; informative text clarifying privacy issues and the need for secured access restrictions would be helpful.

Asset Identification-1: The IoT product can be uniquely identified by the customer and other authorized entities (e.g., the IoT product developer).

The language in Asset Identification-1 includes a limitation on who should have access to any kind of identifier for the devices, i.e., “the customer and other authorized entities.” This limitation is appropriate as some kinds of identifiers are considered personally identifiable information (PII) and cause privacy concerns. There is potential for confusion from the brief statement in Asset Identification-1. Reviewers felt that the language required PII exposure and was not sufficiently clear about the potential privacy risks.

> **Recommendation**: Add informative text explaining the risk of PII exposure when asset identification information is not limited to customers and authorized users.

5 LABELING AND THE NIST CRITERIA

Generally, if the recommendations in Section 4 (*Findings and Recommendations*) are adopted, the binary label structure and informational resources recommended the NIST Criteria can be followed.

As the UL Scheme demonstrates, a tiered label can also be used. Presence or absence of the UL IoT Security Rating Bronze/Silver/Gold/Platinum/Diamond is a binary element. UL provides significant follow-up information on the product itself and on the program for those looking for the additional information recommended by NIST.

Tiering of such information into “Frequently Asked (Consumer) Questions” and material or contact points for more serious security researchers is variously described or implied in the NIST Criteria.

6 REFERENCES

The following reference documents were used in this Pilot.

1. ANSI/CTA-2088, *“Baseline Cybersecurity Standard for Devices and Device Systems”*, December 2020, Consumer Technology Association, https://shop.cta.tech/products/baseline-cybersecurity-standard-for-devices-and-device-systems-cta-2088
2. (Draft) ANSI/CTA-2088-A, “Baseline Cybersecurity Standard for Devices and Device Systems—Revision A”, expected Q1 2022, Consumer Technology Association.
3. *Risk Assessment and Threat Modeling*, Apple Inc., 2012, https://developer.apple.com/library/archive/documentation/Security/Conceptual/Security_Overview/ThreatModeling/ThreatModeling.html, retrieved February 2022.
4. *“The BSA Framework for Secure Software v1.1”*, September 2020, BSA | The Software Alliance, https://www.bsa.org/files/reports/bsa_framework_secure_software_update_2020.pdf
5. ETSI EN 303 645 v2.1.1, *“Cyber Security for Consumer Internet of Things: Baseline Requirements”*, June 2020, ETSI, https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
6. NIST, “*Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products*”, available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf, retrieved 2022-02-11.
7. NIST Special Publication 2000-02, “Conformity Assessment Considerations for Federal Agencies”, https://doi.org/10.6028/NIST.SP.2000-02
8. NISTIR 8259, *“Foundational Cybersecurity Activities for IoT Device Manufacturers”*, May 2020, https://csrc.nist.gov/publications/detail/nistir/8259/final
9. NISTIR 8259A, *“IoT Device Cybersecurity Capability Core Baseline”*, May 2020, https://csrc.nist.gov/publications/detail/nistir/8259a/final
10. NISTIR 8259B, *“IoT Non-Technical Supporting Capability Core Baseline”*, August 2021, https://csrc.nist.gov/publications/detail/nistir/8259b/final
11. NIST, Online Informative Reference Template (Criterial for Consumer IoT Cybersecurity Label version), https://csrc.nist.gov/csrc/media/Projects/olir/documents/Consumer_IoT_Labeling_Focal_Document_Final.xlsx, retrieved 2022-02-11.
12. NIST, *National Online Informative References (OLIR) Program: Submission Guidance for OLIR Developers*, NISTIR 8278A, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8278A.pdf
13. UL IoT Security Rating, https://www.ul.com/services/ul-verified-iot-device-security-rating

14. UL MCV 1376, “Methodology for Marketing Claim Verification: Security Capabilities to Levels Bronze/Silver/Gold/Platinum/Diamond Version 2.0”, September 2021, https://www.shopulstandards.com/ProductDetail.aspx?productId=UL1376_2_A_20210923

15. OMB Circular A-119, https://www.whitehouse.gov/wp-content/uploads/2020/07/revised_circular_a-119_as_of_1_22.pdf

ANNEX A: MAPPING CTA-2088-A AND BSA FRAMEWORK TO THE NIST CRITERIA (OLIR TEMPLATE)

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Asset Identification	The IoT product is uniquely identifiable and inventories all of the IoT product's components.						
Asset Identification-1	The IoT product can be uniquely identified by the customer and other authorized entities (e.g., the IoT product developer).	Functional	equal	[CTA-2088-A] 5.1 Device Identifiers	Recommends a unique value associated with the device ("endpoint",; noting that there may be multiple endpoints in a physical device) that can be referenced without ambiguity.	Y	
Asset Identification-2	The IoT product uniquely identifies each IoT product component and maintains an up-to-date inventory of connected product components.					N	This OLIR mapping is for the hardware component of the IoT product. This functionality would likely be the responsibility of an associated product component such as a smartphone app.
Product Configuration	The configuration of the IoT product is changeable, there is the ability to restore a secure default setting, and any and all changes can only be performed by authorized individuals, services, and other IoT product components.						

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Product Configuration-1	The customer can change the configuration settings of the IoT product via one or more IoT product components.	Semantic	equal	[CTA-2088-A] SA-001 [Device Configuration]	Recommends that the device allow changes to its Configuration.	Y	
Product Configuration-2	The IoT product applies configuration settings to applicable IoT components.					N	This OLIR mapping is for the hardware component of the IoT product. This functionality would likely be the responsibility of an associated product component such as a smartphone app.
Data Protection	The IoT product and its components protect data stored (across all IoT product components) and transmitted (both between IoT product components and outside the IoT product) from unauthorized access, disclosure, and modification.						
Data Protection-1	Each IoT product component protects data it stores via secure means, including the ability to delete or render inaccessible data stored that is either collected from or about the customer, home, family, etc.	Semantic	equal	[CTA-2088-A] Section 5.4 Data at Rest is Protected	Requires that the Confidentiality, Integrity, and Authenticity of data at rest is ensured by sound cryptographic means	Y	See also Section 5.8 Cryptography. This OLIR mapping is for the hardware component of the IoT product. This functionality would likely be the responsibility of an association app product component.
Data Protection-1	Each IoT product component protects data it stores via secure means, including the ability to delete or render inaccessible	Semantic	equal	[CTA-2088-A] Section 5.10 Reprovisioning	Requires that a device can be securely reprovisioned or deprovisioned or users must be notified that secure disposal is required.	Y	This OLIR mapping is for the hardware component of the IoT product. This functionality would likely be the responsibility of an

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
	data stored that is either collected from or about the customer, home, family, etc.						association app product component.
Data Protection-2	When data is sent between IoT product components or outside the product, protections are used for the data transmission.	Semantic	equal	[CTA-2088-A] Section 5.3 Data in Transit is Protected	Requires that the Confidentiality, Integrity, and Authenticity of data in transit is ensured by sound cryptographic means.	Y	See also Section 5.8 Cryptography
Interface Access Control	The IoT product and its components restrict logical access to local and network interfaces – and to protocols and services used by those interfaces – to only authorized individuals, services, and IoT product components.						
Interface Access Control-1	Each IoT product component controls access (to and from) all interfaces (e.g., local interfaces, network interfaces, protocols, and services) in order to limit access to only authorized entities.						
Interface Access Control-1a	Use and have access only to interfaces necessary for the IoT product's operation. All other channels and access to channels are removed or secured.	Semantic	equal	[CTA-2088-A] Section 5.2.3 User Interfaces, Console Ports and Remote Management Protocols	Requires that physical and logical interfaces that may compromise the security of the device are secured, disabled or removed	Y	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Interface Access Control-1b	For all interfaces necessary for the IoT product's use, access control measures are in place (e.g., unique password-based multifactor authentication).	Semantic	subset of	[CTA-2088-A] Section 5.2 Secured Access	Requires securely authenticating and authorizing users, other devices or services for remote, local or physical access to the device	Y	
Interface Access Control-1c	For all interfaces, access and modification privileges are limited.	Semantic	equal	[CTA-2088-A] Section 5.2.3 User Interfaces, Console Ports and Remote Management Protocols	Requires that device configuration privileges, through User Interfaces, Remote Management Protocols or Console Ports are secured	Y	
Interface Access Control-1c	For all interfaces, access and modification privileges are limited.	Semantic	equal	[CTA-2088-A] SA-004 [Diagnostic Ports]	Recommends that diagnostic ports are secured by disabling, limiting features or requiring credentials	Y	
Interface Access Control-2	The IoT product executes means via some, but not necessarily all, components to protect and maintain interface access control.						
Interface Access Control-2a	Validate that data sent to other product components matches specified definitions of format and content.	Semantic	equal	[CTA-2088-A] Section 5.6 Data Validation	Requires that all data transiting into the device is thoroughly validated. Recommends that all data leaving the device is well formed, safe to pass on and as intended	Y	The Interface Access Control-2a requirement for data sent to other product components would be easier to implement if each component had responsibility for its own input, rather than for outputs to other components.

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Interface Access Control-2b	Prevent unauthorized transmissions or access to other product components.	Functional	subset of	[CTA-2088-A] Section 5.2 Secured Access	Requires securely authenticating and authorizing users, other devices or services for remote, local or physical access to the device	Y	This OLIR mapping is for the hardware component of the IoT product. This requirement would be covered by Secure Access and Data In Transit requirements of the reference document.
Interface Access Control-2c	Maintain appropriate access control during initial connection (i.e., on-boarding) and when reestablishing connectivity after disconnection or outage.	Functional	equal	[CTA-2088-A] DI-004 [Bootstrapping Mechanism]	Recommends using an industry standard bootstrapping mechanism for devices without a display and input mechanism	Y	See also Future Secure Capabilities - Section 8.2 Device network Onboarding, planned to be part of the Baseline in the future
Interface Access Control-2c	Maintain appropriate access control during initial connection (i.e., on-boarding) and when reestablishing connectivity after disconnection or outage.	Functional	equal	[CTA-2088-A] SA-002 [Authentication for Admin Access]	Requires successful user authentication for admin or configuration functions	Y	In "Maintain appropriate access control", the word "appropriate is interpreted as covering admin and configuration functions. These are defined in the reference document. No distinction is made between onboarding or reestablishing connectivity; the requirement applies to both. See also DI-004 Bootstrapping Mechanism.
Interface Access Control-2c	Maintain appropriate access control during initial connection (i.e., on-boarding) and when reestablishing connectivity after disconnection or outage.	Functional	equal	[CTA-2088-A] SA-005 [Change Non-Unique Default Credentials on First Use]	Requires credential change for non-unique default credentials upon first use (onboarding)	Y	See also Section 5.24 Web Services

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Software Update	The software of all IoT product components can be updated by authorized individuals, services, and other IoT product components only by using a secure and configurable mechanism, as appropriate for each IoT product component.						
Software Update-1	Each IoT product component can receive, verify, and apply verified software updates.	Functional	subset of	[CTA-2088-A] Section 5.9 Patchability	Requires a secure method for updating firmware or software by authorized entities, post-market. Updates must be authenticated	Y	Note also that PAT-002 [Security of Patch] requires cryptographically secure means to ensure 1) integrity and 2) authenticity
Software Update-2	The IoT product implements measures to keep software on IoT product components up to date (i.e., automatic application of updates or consistent customer notification of available updates via the IoT product).	Semantic	equal	[CTA-2088-A] PAT-004 [Unattended Patching]	Recommends providing users with an option for installation of automatic security patches	Y	
Cybersecurity State Awareness	The IoT product supports detection of cybersecurity incidents affecting or affected by IoT product components and the data they store and transmit.						

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Cybersecurity State Awareness-1	The IoT product captures and records information about the state of IoT components that can be used to detect cybersecurity incidents affecting or affected by IoT product components and the data they store and transmit.	Functional	superset of	[CTA-2088-A] ELG-001 [Event Logging]	Requires the capability to report logging of Security events, but conditioned on certain abilities to actually use such Events.	N	CTA-2088 does not require this capability unless there is a secure management or access feature, such a feature is considered necessary for enterprise product but only recommended for consumer. In other words, for a (consumer) product that will not have an IT manager reading logs, CSA-1 / ELG-001 should not apply.
Documentation	The IoT product developer creates, gathers, and stores information relevant to cybersecurity of the IoT product and its product components prior to customer purchase, and throughout the development of a product and its subsequent lifecycle.						
Documentation-1	Throughout the development lifecycle, the IoT product developer creates or gathers and stores information relevant to the cybersecurity of the IoT product and its product components						
Documentation-1a	Assumptions made during the development process and other expectations related to the IoT product						

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Documentation-1a(i)	Expected customers and use cases.	Functional	superset of	[BSA] SC.1-1	"SC.1-1. Software development organizations document likely threats." Threat analysis requires documentation and understanding of this information.	N	The cybersecurity purpose of this specific information isn't entirely clear. A threat is valid regardless of who purchases the product. To the extent that this informs threat modeling, however, this information is typically collected in process flow diagramming in threat modelling.
Documentation-1a(ii)	Physical use, including security of the location of the IoT product and its product components (e.g., a camera for use inside the home which has an off switch on the device vs. a security camera for use outside the home which does not have an off switch on the device), and characteristics.	Functional	subset of	[BSA] SC.1-1	"SC.1-1. Software development organizations document likely threats." Threat analysis requires documentation and understanding of this information.	Y	
Documentation-1a(iii)	Network access and requirements (e.g., bandwidth requirements).	Functional	subset of	[BSA] SC.1-1	"SC.1-1. Software development organizations document likely threats." Threat analysis requires documentation and understanding of this information.	Y	
Documentation-1a(iv)	Data created and handled by the IoT product.	Functional	subset of	[BSA] SC.2-2	"SC.2-2. Software uses canonical data formats." When deciding on specifics of canonical data formats, the type of data collected and the storage format must be determined.	Y	
Documentation-1a(v)	Any expected data inputs and outputs (including error codes, frequency,	Functional	subset of	[BSA] SC.2-2	"SC.2-2. Software uses canonical data formats." When deciding on specifics of canonical data	Y	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
	type/form, range of acceptable values, etc.).				formats, the data inputs and outputs must be determined.		
Documentation-1a(vi)	The IoT product developer's assumed cybersecurity requirements for the IoT product.	Functional	equal	[BSA] SC.1-2	"SC.1-2. Threats are rated and prioritized according to risk."	Y	
Documentation-1a(vii)	Any laws and regulations with which the IoT product and related support activities comply.	Syntactic	not related to	[BSA] SC.1-2	"SC.1-2. Threats are rated and prioritized according to risk."	N	Documenting the laws and regulations is an important business process which can inform the product requirements and will influence the cybersecurity requirements planning, but it should not be made part of the Scheme.
Documentation-1a(viii)	Expected lifespan and anticipated cybersecurity costs related to the IoT product (e.g., price of maintenance), and length and terms of support.	Syntactic	not related to	[BSA] SC.1-2	"SC.1-2. Threats are rated and prioritized according to risk."	N	Much of this information is important to the business planners in the manufacturing organization but does not address cybersecurity threats. Support terms are dealt with in warranty agreements and out-of-scope for a conformity scheme.
Documentation-1b	All IoT components, including but not limited to the IoT device, that are part of the IoT product.		not related to			N	This mapping pertains to the hardware device. The device may be bundled with or connected to a variety of other components.

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Documentation-1c	How the baseline product criteria are met by the IoT product across its product components, including which baseline product criteria are not met by IoT product components and why (e.g., the capability is not needed based on risk assessment).		not related to			N	This mapping pertains to the hardware device. The device may be bundled with or connected to a variety of other components.
Documentation-1d	Product design and support considerations related to the IoT product, for example: i. 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). ii. IoT platform used in the development and operation of the IoT product, its product components, including related documentation. iii. Protection of software and hardware elements implemented to create the IoT product and its product components (e.g., secure boot, hardware root of trust, and secure enclave). iv. Consideration of	Functional	superset of	[BSA] SC.1-2	"SC.1-2. Threats are rated and prioritized according to risk."	N	As worded, this item could lead to a requirement for SBOM. While SBOM shows promise in NTIA- and CISA-led efforts and in proof-of-concept exercises, wide-scale piloting would be appropriate before including as a baseline requirement. Some of the other items are not well-suited for incident response, such as (iv), which may be a concern for liability reasons; (vi), which may be useful in strengthening future efforts but not of use in incident response; and (vii) which has to do with product planning and requirements.

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
	the known risks related to the IoT product and known potential misuses. v. Secure software development and supply chain practices used. vi. Accreditation, certification, and/or evaluation results for cybersecurity-related practices. vii. The ease of installation and maintenance of the IoT product by a customer (i.e., the usability of the product [ISO9241]).						
Documentation-1e	Maintenance requirements for the IoT product, for example: i. Cybersecurity maintenance expectations and associated instructions or procedures (e.g., vulnerability/patch management plan). ii. How the IoT product developer identifies authorized supporting parties who can perform maintenance activities (e.g., authorized repair centers). iii. Cybersecurity considerations of the	Functional	intersects with	[BSA] PA.1	a) PA.1. Software is capable of receiving secure updates and security patches.	N	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
	maintenance process (e.g., how customer data unrelated to the maintenance process remains confidential even from maintainers).						
Documentation-1f	The secure system lifecycle policies and processes associated with the IoT product	Semantic	equal	[BSA] The BSA Framework for Secure Software v1.1	The Framework covers secure system lifecycle policies and processes for IoT product design.	Y	
Documentation-1f(i)	Steps taken during development to ensure the IoT product and its product components are free of any known, exploitable vulnerabilities.	Semantic	equal	[BSA] SC.3-1	Software avoids, or includes documented mitigations for, known security vulnerabilities in included functions and libraries.	Y	
Documentation-1f(ii)	The process of working with component suppliers and third-party vendors to ensure the security of the IoT product and its product components is maintained for the duration of its supported lifecycle.	Semantic	superset of	[BSA] SM.1-1	An organizational supply chain management plan and processes for identification and reporting of supply chain incidents are established.	N	If grouping is supported, items here for Documentation-1f(ii) can be grouped together. In that case, the "Fulfilled by" status should be changed to "Y".
Documentation-1f(ii)	The process of working with component suppliers and third-party vendors to ensure the security of the IoT product and its product components is maintained for the duration of its supported lifecycle.	Semantic	superset of	[BSA] SM.2-1	Information about providers of thirdparty components is identified and collected.	N	If grouping is supported, items here for Documentation-1f(ii) can be grouped together. In that case, the "Fulfilled by" status should be changed to "Y".

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Documentation-1f(ii)	The process of working with component suppliers and third-party vendors to ensure the security of the IoT product and its product components is maintained for the duration of its supported lifecycle.	Semantic	superset of	[BSA] SM.2-2	Software development organization employs measures to document and, to the extent feasible, trace to their original source all third-party components directly acquired and incorporated into the software by the developer.	N	If grouping is supported, items here for Documentation-1f(ii) can be grouped together. In that case, the "Fulfilled by" status should be changed to "Y".
Documentation-1f(ii)	The process of working with component suppliers and third-party vendors to ensure the security of the IoT product and its product components is maintained for the duration of its supported lifecycle.	Semantic	superset of	[BSA] SM.2-3	To the maximum feasible through the use of manual and automated technologies, subcomponents integrated in thirdparty components are documented, and their lineage and dependencies traced.	N	If grouping is supported, items here for Documentation-1f(ii) can be grouped together. In that case, the "Fulfilled by" status should be changed to "Y".
Documentation-1f(ii)	The process of working with component suppliers and third-party vendors to ensure the security of the IoT product and its product components is maintained for the duration of its supported lifecycle.	Semantic	superset of	[BSA] SM.2-4	Security requirements are incorporated into contracts, policies, and standards for vendors supplying software components.	N	If grouping is supported, items here for Documentation-1f(ii) can be grouped together. In that case, the "Fulfilled by" status should be changed to "Y".

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Documentation-1f(iii)	Any post end-of-support considerations, such as the discovery of a vulnerability which would significantly impact the security, privacy, or safety of customers who continue to use the IoT product and its product components.	Functional	intersects with	[BSA] EL.1	a) EL.1. Vendor maintain consistent lifecycle guidance. i) EL.1-1. Vendor communicates realistic assumptions and expectations regarding the nature and lifespan of product support in tandem with initial software delivery. ii) EL.1-2. Vendor clearly communicates decisions to terminate support for a software product to customers and users, identifying the expected support termination date; the anticipated risk of continued product use beyond the termination of support; possible mitigation actions; and options for technical migration to replacement products. iii) EL.1-3. Software is continually monitored to ensure that third-party components have not reached end-of-life milestones or are removed or otherwise remediated.	N	The function of this requirement is unclear. If the manufacturer is no longer providing support, then it takes no action. This implies that the customer takes action as they see fit, leading this requirement to be essentially the same for every product.
Documentation-1g	The vulnerability management policies and processes associated with the IoT product	Semantic	equal	[BSA] VM.1	The vendor maintains an up-to-date vulnerability management plan.	Y	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Documentation-1g(i)	Methods of receiving reports of vulnerabilities (see Information and Query Reception below).	Semantic	subset of	[BSA] VM.3	The vendor maintains a coordinated vulnerability disclosure program. (This group includes requirements for an intake mechanism to receive reports; a published policy with a number of details; tracking; and reporting on mitigation.)	Y	
Documentation-1g(ii)	Processes for recording reported vulnerabilities.	Semantic	equal	[BSA] VM3.-4	The vendor maintains a system to record and track all reports of potential vulnerabilities.	Y	
Documentation-1g(iii)	Policy for responding to reported vulnerabilities, including the process of coordinating vulnerability response activities among component suppliers and third-party vendors.	Semantic	subset of	[BSA] VM.3-3	The vendor publishes, in simple and clear language, its policies for interacting with vulnerability reporters, addressing, at minimum (group continues with a list of required policy elements).	Y	
Documentation-1g(iv)	Policy for disclosing reported vulnerabilities.	Functional	subset of	[BSA] SM.1-1	An organizational supply chain management plan and processes for identification and reporting of supply chain incidents are established.	Y	
Documentation-1g(v)	Processes for receiving notification from component suppliers and third-party vendors about any change in the status of their supplied components, such as end of production, end of support, deprecated status (e.g., the product is no longer recommended for use), or known insecurities.	Semantic	superset of	[BSA] EL.1-3	Software is continually monitored to ensure that third-party components have not reached end-of-life milestones or are removed or otherwise remediated.	N	If grouping is supported, items here for Documentation-1g(v) can be grouped together. In that case, the "Fulfilled by" status should be changed to "Y".

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Documentation-1g(v)	Processes for receiving notification from component suppliers and third-party vendors about any change in the status of their supplied components, such as end of production, end of support, deprecated status (e.g., the product is no longer recommended for use), or known insecurities.	Semantic	superset of	[BSA] VM.1-3	The vulnerability management plan includes a process for gaining timely awareness of and managing vulnerabilities that are discovered in third-party components of the software.	N	If grouping is supported, items here for Documentation-1g(v) can be grouped together. In that case, the "Fulfilled by" status should be changed to "Y".
Information and Query Reception	The ability of the IoT product developer to receive information relevant to cybersecurity and respond to queries from the customer and others about information relevant to cybersecurity.						
Information and Query Reception-1	The IoT product developer can receive information related to the cybersecurity of the IoT product and its product components and can respond to queries related to cybersecurity of the IoT product and its product components from customers and others						
Information and Query Reception-1a	The ability of the IoT product developer to identify a point of contact to receive maintenance and vulnerability information (e.g., bug reporting capabilities and bug bounty programs) from customers	Semantic	equal	[BSA] VM.3-1	The vendor establishes a clearly defined and easily accessible intake mechanism to accept vulnerability information (email, portal, etc.).	Y	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
	and others in the IoT product ecosystem (e.g., repair technician acting on behalf of the customer).						
Information and Query Reception-1b	The ability of the IoT product developer to receive queries from and respond to customers and others in the IoT product ecosystem about the cybersecurity of the IoT product and its components.	Semantic	equal	[BSA] VM.3-1	The vendor establishes a clearly defined and easily accessible intake mechanism to accept vulnerability information (email, portal, etc.).	Y	
Information Dissemination	The IoT product developer broadcasts (e.g., to the public) and distributes (e.g., to the customer or others in the IoT product ecosystem) information relevant to cybersecurity.						
Information Dissemination-1	The IoT product developer can broadcast to many/all entities via a channel (e.g., a post on a public channel) to alert the public and customers of the IoT product about cybersecurity relevant information and events throughout the support lifecycle.	Semantic	intersects with	[BSA] VN.3	Patches or updates for security issues are accompanied by advisory messages informing users of relevant information.	N	The Framework does not require that vulnerabilities be advertised to the public, just to customers/users, and as part of patch documentation.

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Information Dissemination-1a	Updated terms of support (e.g., frequency of updates and mechanism(s) of application) and notice of availability and/or application of software updates.					N	Terms of support are a commerical issue. As written, this item does not directly address cybersecurity. In consumer products, updates are typically provided when the security team identifies and remediates a vulnerability, not acccording to terms of support.
Information Dissemination-1a	Updated terms of support (e.g., frequency of updates and mechanism(s) of application) and notice of availability and/or application of software updates.	Semantic	subset of	[BSA] VN	The VN section covers notice of availability and/or application of software updates.	Y	"Fulfilled By" excludes "updated terms of support", which should be out-of-scope for the Criteria.
Information Dissemination-1b	End of term of support or functionality for the IoT product.	Semantic	equal	[BSA] EL.1-2	Vendor clearly communicates decisions to terminate support for a software product to customers and users, identifying the expected support termination date; the anticipated risk of continued product use beyond the termination of support; possible mitigation actions; and options for technical migration to replacement products.	Y	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Information Dissemination-1c	Needed maintenance operations.	Functional	equal	[BSA] VN.3	Patches or updates for security issues are accompanied by advisory messages informing users of relevant information.	Y	The Criteria text does not call out "maintenance" in the context of security updates or vulnerability issues. However, in the context of the purpose of the Criteria, it seems reasonable to limit the scope of the requirement to cybersecurity.
Information Dissemination-1d	New IoT device vulnerabilities, associated details, and mitigation actions needed from the customer.	Functional	intersects with	[BSA] VN.1	Patches or updates for security issues are accompanied by advisory messages informing users of relevant information.	N	This Criteria does not distinguish between critical, public-disclosure-worthy vulnerabilities and those requiring no action.
Information Dissemination-1e	Breach discovery related to an IoT product and its product components used by the customers, associated details, and mitigation actions needed from the customer (if any).	Functional	equal	[BSA] VN.3-1	Users are notified of a significant security issue when a remediation is in place for each supported version of the affected product.	Y	There is a functional difference in that the BSA Framework presumes the notification occurs when the remediation is available.

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Information Dissemination-2	The IoT product developer can distribute information relevant to cybersecurity of the IoT product and its product components to alert appropriate ecosystem entities (e.g., common vulnerability tracking authorities, accreditors and certifiers, third-party support and maintenance organizations) about cybersecurity relevant information, for example: a. Applicable documentation captured during the design and development of the IoT product and its product components. b. Cybersecurity and vulnerability alerts and information about resolution of any vulnerability. c. An overview of the information security practices and safeguards used by the IoT product developer. d. Accreditation, certification, and/or evaluation results for the IoT product developer's cybersecurity-related practices. e. A risk assessment	Functional	superset of	[BSA] VN	The Vulnerability Notification section of the BSA Framework covers security and vulnerability alerts and information about resolution.	N	Item (a) refers back to the Documentation section, which is overly broad. Items (c), (d), and (e) do not appear to serve a cybersecurity purpose.

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
	report or summary for the IoT product developer's business environment risk posture.						
Product Education and Awareness	The IoT product developer creates awareness of and educates customers and others in the IoT product ecosystem about cybersecurity-related information (e.g., considerations, features) related to the IoT product and its product components.						
Product Education and Awareness-1	The IoT product developer creates awareness and provides education targeted at customers about information relevant to cybersecurity of the IoT product and its product components						

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Product Education and Awareness-1a	The presence and use of IoT product cybersecurity capabilities					N	
Product Education and Awareness-1a(i)	How to change configuration settings and the cybersecurity implications of changing settings, if any.	Semantic	equal	[BSA] CF.1-3	The software documentation describes configurations and procedures for secure configuration under normal operation.	Y	
Product Education and Awareness-1a(ii)	How to configure and use access control functionality (e.g., set and change passwords).	Semantic	subset of	[BSA] CF.1-3	The software documentation describes configurations and procedures for secure configuration under normal operation.	Y	It is not clear how access control functionality is separate from configuration settings.
Product Education and Awareness-1a(iii)	How software updates are applied and any instructions necessary for the customer on how to use software update functionality.	Semantic	equal	[BSA] VN.3-2	Advisory messages notifying users of security issues include information on affected products, applicable versions, and platforms; a unique identification number; and a brief description of the vulnerability and its potential impact.	Y	
Product Education and Awareness-1a(iv)	How to manage device data including creation, update and deletion of data on the IoT product.					N	
Product Education and Awareness-1b	How to maintain the IoT product and its product components during its lifetime, including after the period of security support (e.g., delivery of software updates and patches) from the IoT product developer.					N	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Product Education and Awareness-1c	How an IoT product and its product components can be securely re-provisioned or disposed of.	Semantic	equal	[BSA] CTA-2088 REP-001	At least one Field Deprovisioning procedure that includes Secure Purge or Destroy operations (as defined in NIST SP 800-88 Rev.1 [13]), Cryptographic Erasure, or physical removal of the media containing user-specific data shall be provided in a place and manner available to expected authorized users.	Y	
Product Education and Awareness-1d	Vulnerability management options (e.g., configuration and patch management and anti-malware) available for the IoT product or its product components that could be used by customers.	Functional	intersects with	[BSA] VN.3-2	Advisory messages notifying users of security issues include information on affected products, applicable versions, and platforms; a unique identification number; and a brief description of the vulnerability and its potential impact.	N	
Product Education and Awareness-1e	Additional information customers 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).						Terms of support are a commercial issue and will be addressed in warranty documentation and updates.

ANNEX B: MAPPING UL MCV 1376 / UL IOT SECURITY RATING TO THE NIST CRITERIA (OLIR TEMPLATE)

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Asset Identification	The IoT product is uniquely identifiable and inventories all of the IoT product's components.						
Asset Identification-1	The IoT product can be uniquely identified by the customer and other authorized entities (e.g., the IoT product developer).	Semantic	Subset of	[UL-MCV-1376] 6.6.1 PD-DEVID - Product Identification	The model designation of the device must be available to the end user The device must have an identifier that uniquely identifies it. Additionally, the device must have the capability to show the currently running firmware version to the end-user.	Y	
Asset Identification-2	The IoT product uniquely identifies each IoT product component and maintains an up-to-date inventory of connected product components.	Semantic	Superset of	[UL-MCV-1376] 6.6.1 PD-DEVID - Product Identification	A device identifier may be put on the device itself in physical form (such as a printed or etched label) or it may be accessible through a network API (such as a web interface or companion app). Due to the nature of the firmware version and its volatility, it needs to be available through some form of HMI (e.g., an app or a display), and having it printed on the device itself is not sufficient.	N	This OLIR mapping is for the hardware component of the IoT product. As such this NIST criteria is fulfilled for the hardware device, but not other components such as Cloud, software, etc.

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Product Configuration	The configuration of the IoT product is changeable, there is the ability to restore a secure default setting, and any and all changes can only be performed by authorized individuals, services, and other IoT product components.						
Product Configuration-1	The customer can change the configuration settings of the IoT product via one or more IoT product components.	Semantic	Subset of	[UL-MCV-1376] 6.3.2 LS-SECDEF - Systems configured to secure defaults	The default configuration of the system must ensure that the device is secure "out of the box"	Y	UL MCV 1376 defines the requirements for a secure default configuration, as well as the security requirements involved for a customer to change from these default configurations.
Product Configuration-2	The IoT product applies configuration settings to applicable IoT components.					N	This OLIR mapping is for the hardware component of the IoT product. This functionality would likely be the responsibility of an associated product component such as a smartphone app.
Data Protection	The IoT product and its components protect data stored (across all IoT product components) and transmitted (both between IoT product components and outside the IoT product) from unauthorized access, disclosure, and modification.						

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Data Protection-1	Each IoT product component protects data it stores via secure means, including the ability to delete or render inaccessible data stored that is either collected from or about the customer, home, family, etc.	Semantic	equal	[UL MCV 1376] 6.4.2 SM - ERASE: Permanent erasure of sensitive data	Permanent erasure of sensitive data must be supported	Y	See also Section 5.8 Cryptography. This OLIR mapping is for the hardware component of the IoT product. This functionality would likely be the responsibility of an association app product component.
Data Protection-2	When data is sent between IoT product components or outside the product, protections are used for the data transmission.	Semantic	Subset of	[UL MCV 1376] 6.5.1 CS-XMIT - Cryptographically secure data transmission	Communication channels need to be protected via cryptographic means to achieve various security properties	Y	
Interface Access Control	The IoT product and its components restrict logical access to local and network interfaces – and to protocols and services used by those interfaces – to only authorized individuals, services, and IoT product components.						
Interface Access Control-1	Each IoT product component controls access (to and from) all interfaces (e.g., local interfaces, network interfaces, protocols, and services) in order to limit access to only authorized entities.	Semantic	Subset of	[UL MCV 1376] 6.2.1 DC-NDK - No default credentials or secret keys 6.2.3 DC-PWD - Passpharse complexity enforcement 6.4.1 SM-AUTH - Sensitive services requrie authentication	6.2.1: System defaults such as password and/or cryptographic keys must be changed on the initial setup 6.2.3: When passphrases are used to authorize the use of services, they must fulfill minimum strength criteria 6.4.1: Sensitive services must require authentication and ensure the confidentiality and integrity of data		

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Interface Access Control-1a	Use and have access only to interfaces necessary for the IoT product's operation. All other channels and access to channels are removed or secured.	Semantic	Subset of	[UL MCV 1376] 6.2.1 DC-NDK - No default credentials or secret keys 6.2.3 DC-PWD - Passpharse complexity enforcement 6.4.1 SM-AUTH - Sensitive services requrie authentication	6.2.1: System defaults such as password and/or cryptographic keys must be changed on the initial setup 6.2.3: When passphrases are used to authorize the use of services, they must fulfill minimum strength criteria 6.4.1: Sensitive services must require authentication and ensure the confidentiality and integrity of data	Y	
Interface Access Control-1b	For all interfaces necessary for the IoT product's use, access control measures are in place (e.g., unique password-based multifactor authentication).	Semantic	subset of	[UL MCV 1376] 6.2.1 DC-NDK - No default credentials or secret keys 6.2.3 DC-PWD - Passpharse complexity enforcement 6.4.1 SM-AUTH - Sensitive services requrie authentication	6.2.1: System defaults such as password and/or cryptographic keys must be changed on the initial setup 6.2.3: When passphrases are used to authorize the use of services, they must fulfill minimum strength criteria 6.4.1: Sensitive services must require authentication and ensure the confidentiality and integrity of data	Y	
Interface Access Control-1c	For all interfaces, access and modification privileges are limited.	Semantic	Subset of	[UL MCV 1376] 6.2.1 DC-NDK - No default credentials or secret keys 6.2.3 DC-PWD - Passpharse complexity enforcement 6.4.1 SM-AUTH - Sensitive services	6.2.1: System defaults such as password and/or cryptographic keys must be changed on the initial setup 6.2.3: When passphrases are used to authorize the use of services, they must fulfill minimum strength criteria 6.4.1: Sensitive services must require authentication and	Y	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
				requrie authentication	ensure the confidentiality and integrity of data		
Interface Access Control-1c	For all interfaces, access and modification privileges are limited.	Semantic	Subset of	[UL MCV 1376] 6.2.1 DC-NDK - No default credentials or secret keys 6.2.3 DC-PWD - Passpharse complexity enforcement 6.4.1 SM-AUTH - Sensitive services requrie authentication	6.2.1: System defaults such as password and/or cryptographic keys must be changed on the initial setup 6.2.3: When passphrases are used to authorize the use of services, they must fulfill minimum strength criteria 6.4.1: Sensitive services must require authentication and ensure the confidentiality and integrity of data	Y	
Interface Access Control-2	The IoT product executes means via some, but not necessarily all, components to protect and maintain interface access control.						
Interface Access Control-2a	Validate that data sent to other product components matches specified definitions of format and content.						
Interface Access Control-2b	Prevent unauthorized transmissions or access to other product components.						

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Interface Access Control-2c	Maintain appropriate access control during initial connection (i.e., on-boarding) and when reestablishing connectivity after disconnection or outage.						
Interface Access Control-2c	Maintain appropriate access control during initial connection (i.e., on-boarding) and when reestablishing connectivity after disconnection or outage.						
Interface Access Control-2c	Maintain appropriate access control during initial connection (i.e., on-boarding) and when reestablishing connectivity after disconnection or outage.						
Software Update	The software of all IoT product components can be updated by authorized individuals, services, and other IoT product components only by using a secure and configurable mechanism, as appropriate for each IoT product component.						

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Software Update-1	Each IoT product component can receive, verify, and apply verified software updates.	Semantic	equal	[UL MCV 1376] 6.1.3 SWU-AUT - Software update authentication	Software updates must be cryptographically authenticated, and provide anti-rollback features	Y	
Software Update-2	The IoT product implements measures to keep software on IoT product components up to date (i.e., automatic application of updates or consistent customer notification of available updates via the IoT product).	Semantic	Subset of	[UL MCV 1376] 6.1.1 SWU-SUPP - Remote Software updates supported 6.1.2 SWU-AUTO - Automatic software update tracking	6.1.1: Software updates must be supported, using network or wireless interfaces where available 6.1.2: Automatic querying of devices for available software updates must be enabled by default	Y	
Cybersecurity State Awareness	The IoT product supports detection of cybersecurity incidents affecting or affected by IoT product components and the data they store and transmit.						
Cybersecurity State Awareness-1	The IoT product captures and records information about the state of IoT components that can be used to detect cybersecurity incidents affecting or affected by IoT product components and the data they store and transmit.						

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Documentation	The IoT product developer creates, gathers, and stores information relevant to cybersecurity of the IoT product and its product components prior to customer purchase, and throughout the development of a product and its subsequent lifecycle.						
Documentation-1	Throughout the development lifecycle, the IoT product developer creates or gathers and stores information relevant to the cybersecurity of the IoT product and its product components						
Documentation-1a	Assumptions made during the development process and other expectations related to the IoT product						
Documentation-1a(i)	Expected customers and use cases.						
Documentation-1a(ii)	Physical use, including security of the location of the IoT product and its product components (e.g., a camera for use inside the home which has an off switch on the device vs. a security camera for use						

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
	outside the home which does not have an off switch on the device), and characteristics.						
Documentation-1a(iii)	Network access and requirements (e.g., bandwidth requirements).						
Documentation-1a(iv)	Data created and handled by the IoT product.						
Documentation-1a(v)	Any expected data inputs and outputs (including error codes, frequency, type/form, range of acceptable values, etc.).						
Documentation-1a(vi)	The IoT product developer's assumed cybersecurity requirements for the IoT product.						
Documentation-1a(vii)	Any laws and regulations with which the IoT product and related support activities comply.						
Documentation-1a(viii)	Expected lifespan and anticipated cybersecurity costs related to the IoT product (e.g., price of maintenance), and length and terms of support.						

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Documentation-1b	All IoT components, including but not limited to the IoT device, that are part of the IoT product.						
Documentation-1c	How the baseline product criteria are met by the IoT product across its product components, including which baseline product criteria are not met by IoT product components and why (e.g., the capability is not needed based on risk assessment).	Semantic	Intersects with	[UL MCV 1376] 6.6.2 PD-COLL: Data Collection and Handling	Data collection by the device must be documented	N	This mapping pertains to the hardware device. The device may be bundled with or connected to a variety of other components.
Documentation-1d	Product design and support considerations related to the IoT product, for example: i. 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). ii. IoT platform used in the development and operation of the IoT product, its product components, including related documentation. iii. Protection of software and hardware elements implemented to create the IoT product and its product components						

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
	(e.g., secure boot, hardware root of trust, and secure enclave). iv. Consideration of the known risks related to the IoT product and known potential misuses. v. Secure software development and supply chain practices used. vi. Accreditation, certification, and/or evaluation results for cybersecurity-related practices. vii. The ease of installation and maintenance of the IoT product by a customer (i.e., the usability of the product [ISO9241]).						
Documentation-1e	Maintenance requirements for the IoT product, for example: i. Cybersecurity maintenance expectations and associated instructions or procedures (e.g., vulnerability/patch management plan). ii. How the IoT product developer identifies authorized supporting parties who can perform maintenance activities (e.g., authorized repair centers). iii. Cybersecurity						

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
	considerations of the maintenance process (e.g., how customer data unrelated to the maintenance process remains confidential even from maintainers).						
Documentation-1f	The secure system lifecycle policies and processes associated with the IoT product						
Documentation-1f(i)	Steps taken during development to ensure the IoT product and its product components are free of any known, exploitable vulnerabilities.						
Documentation-1f(ii)	The process of working with component suppliers and third-party vendors to ensure the security of the IoT product and its product components is maintained for the duration of its supported lifecycle.						
Documentation-1f(ii)	The process of working with component suppliers and third-party vendors to ensure the security of the IoT product and its product components is maintained for the duration of its supported lifecycle.						

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Documentation-1f(ii)	The process of working with component suppliers and third-party vendors to ensure the security of the IoT product and its product components is maintained for the duration of its supported lifecycle.						
Documentation-1f(ii)	The process of working with component suppliers and third-party vendors to ensure the security of the IoT product and its product components is maintained for the duration of its supported lifecycle.						
Documentation-1f(ii)	The process of working with component suppliers and third-party vendors to ensure the security of the IoT product and its product components is maintained for the duration of its supported lifecycle.						

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Documentation-1f(iii)	Any post end-of-support considerations, such as the discovery of a vulnerability which would significantly impact the security, privacy, or safety of customers who continue to use the IoT product and its product components.	Semantic	Intersects with	[UL MCV 1376] 6.6.4 PD-EOL: End of life policy	Information on the minimum support period must be available to end-users	N	
Documentation-1g	The vulnerability management policies and processes associated with the IoT product	Semantic	Subset of	[UL MCV 1376] 6.6.5 PD-VMGMT: Vulnerability management program	A vulnerability and disclosure program must be maintained	Y	
Documentation-1g(i)	Methods of receiving reports of vulnerabilities (see Information and Query Reception below).	Semantic	subset of	[UL MCV 1376] 6.6.5 PD-VMGMT: Vulnerability management program	A vulnerability and disclosure program must be maintained	Y	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Documentation-1g(ii)	Processes for recording reported vulnerabilities.	Semantic	Subset of	[UL MCV 1376] 6.6.5 PD-VMGMT: Vulnerability management program	A vulnerability and disclosure program must be maintained	Y	
Documentation-1g(iii)	Policy for responding to reported vulnerabilities, including the process of coordinating vulnerability response activities among component suppliers and third-party vendors.	Semantic	Subset of	[UL MCV 1376] 6.6.5 PD-VMGMT: Vulnerability management program	A vulnerability and disclosure program must be maintained	Y	
Documentation-1g(iv)	Policy for disclosing reported vulnerabilities.	Semantic	Subset of	[UL MCV 1376] 6.6.5 PD-VMGMT: Vulnerability management program	A vulnerability and disclosure program must be maintained	Y	
Documentation-1g(v)	Processes for receiving notification from component suppliers and third-party vendors about any change in the status of their supplied components, such as end of production, end of support, deprecated status (e.g., the product is no longer recommended for use), or known insecurities.	Semantic	Subset of	[UL MCV 1376] 6.6.5 PD-VMGMT: Vulnerability management program	A vulnerability and disclosure program must be maintained	Y	
Documentation-1g(v)	Processes for receiving notification from component suppliers and third-party vendors about any change in the status of their supplied components, such as end of production,	Semantic	Subset of	[UL MCV 1376] 6.6.5 PD-VMGMT: Vulnerability management program	A vulnerability and disclosure program must be maintained	Y	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
	end of support, deprecated status (e.g., the product is no longer recommended for use), or known insecurities.						
Information and Query Reception	The ability of the IoT product developer to receive information relevant to cybersecurity and respond to queries from the customer and others about information relevant to cybersecurity.						
Information and Query Reception-1	The IoT product developer can receive information related to the cybersecurity of the IoT product and its product components and can respond to queries related to cybersecurity of the IoT product and its product components from customers and others	Semantic	Subset of	[UL MCV 1376] 6.6.5 PD-VMGMT: Vulnerability management program	A vulnerability and disclosure program must be maintained	Y	
Information and Query Reception-1a	The ability of the IoT product developer to identify a point of contact to receive maintenance and vulnerability information (e.g., bug reporting capabilities and bug bounty programs) from customers and others in the IoT product ecosystem (e.g., repair technician acting on behalf of the customer).	Semantic	Subset of	[UL MCV 1376] 6.6.5 PD-VMGMT: Vulnerability management program	A vulnerability and disclosure program must be maintained	Y	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Information and Query Reception-1b	The ability of the IoT product developer to receive queries from and respond to customers and others in the IoT product ecosystem about the cybersecurity of the IoT product and its components.	Semantic	Subset of	[UL MCV 1376] 6.6.5 PD-VMGMT: Vulnerability management program	A vulnerability and disclosure program must be maintained	Y	
Information Dissemination	The IoT product developer broadcasts (e.g., to the public) and distributes (e.g., to the customer or others in the IoT product ecosystem) information relevant to cybersecurity.						
Information Dissemination-1	The IoT product developer can broadcast to many/all entities via a channel (e.g., a post on a public channel) to alert the public and customers of the IoT product about cybersecurity relevant information and events throughout the support lifecycle.						
Information Dissemination-1a	Updated terms of support (e.g., frequency of updates and mechanism(s) of application) and notice of availability and/or application of software updates.						

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Information Dissemination-1a	Updated terms of support (e.g., frequency of updates and mechanism(s) of application) and notice of availability and/or application of software updates.						
Information Dissemination-1b	End of term of support or functionality for the IoT product.						
Information Dissemination-1c	Needed maintenance operations.						
Information Dissemination-1d	New IoT device vulnerabilities, associated details, and mitigation actions needed from the customer.						
Information Dissemination-1e	Breach discovery related to an IoT product and its product components used by the customers, associated details, and mitigation actions needed from the customer (if any).						

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Information Dissemination-2	The IoT product developer can distribute information relevant to cybersecurity of the IoT product and its product components to alert appropriate ecosystem entities (e.g., common vulnerability tracking authorities, accreditors and certifiers, third-party support and maintenance organizations) about cybersecurity relevant information, for example: a. Applicable documentation captured during the design and development of the IoT product and its product components. b. Cybersecurity and vulnerability alerts and information about resolution of any vulnerability. c. An overview of the information security practices and safeguards used by the IoT product developer. d. Accreditation, certification, and/or evaluation results for the IoT product developer's cybersecurity-related practices. e. A risk assessment						

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
	report or summary for the IoT product developer's business environment risk posture.						
Product Education and Awareness	The IoT product developer creates awareness of and educates customers and others in the IoT product ecosystem about cybersecurity-related information (e.g., considerations, features) related to the IoT product and its product components.						
Product Education and Awareness-1	The IoT product developer creates awareness and provides education targeted at customers about information relevant to cybersecurity of the IoT product and its product components						

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Product Education and Awareness-1a	The presence and use of IoT product cybersecurity capabilities						
Product Education and Awareness-1a(i)	How to change configuration settings and the cybersecurity implications of changing settings, if any.						
Product Education and Awareness-1a(ii)	How to configure and use access control functionality (e.g., set and change passwords).						
Product Education and Awareness-1a(iii)	How software updates are applied and any instructions necessary for the customer on how to use software update functionality.						
Product Education and Awareness-1a(iv)	How to manage device data including creation, update and deletion of data on the IoT product.						
Product Education and Awareness-1b	How to maintain the IoT product and its product components during its lifetime, including after the period of security support (e.g., delivery of software updates and patches) from the IoT product developer.						

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
Product Education and Awareness-1c	How an IoT product and its product components can be securely re-provisioned or disposed of.						
Product Education and Awareness-1d	Vulnerability management options (e.g., configuration and patch management and anti-malware) available for the IoT product or its product components that could be used by customers.						
Product Education and Awareness-1e	Additional information customers 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).						

ABOUT THE PARTNERS

Consumer Technology Association (CTA)

As North America's largest technology trade association, CTA® is the tech sector. Our members are the world's leading innovators – from startups to global brands – helping support more than 18 million American jobs. CTA owns and produces CES® – the most influential tech event in the world. Find us at CTA.tech. Follow us @CTAtech.

UL Inc.

As the global safety science leader, UL helps companies to demonstrate safety, enhance sustainability, strengthen security, deliver quality, manage risk and achieve regulatory compliance.

SpireSpark International Ltd.

SpireSpark is a consulting firm specializing in the development of conformity assessment programs and has done extensive research on IoT security standards in the UK, EU and US. More information is available at https://spirespark.com/.