Comments on the "Appropriate Definitive Text"

In order to facilitate conformity assessment, the definitive text should be expressed as clear and unambiguous requirements. This serves all market participants by allowing any manufacturer, test lab, or other assessor to arrive at a consistent determination of conformity for a given product and allows the label to be granted fairly and equitably across products in each category of the market. Having more than one label (more than one set of requirements) for a product category will only (1) confuse customers who are attempting to compare products, and (2) lead to some manufacturers choosing the label that is easier to obtain.

Further, the market benefits greatly when these requirements are harmonized globally.

ETSI TC CYBER has already defined clear and unambiguous requirements for consumer IoT devices suitable for conformity assessment and has published European standards in this area; these standards are the planned basis for UK regulation [DCMS] as well as European assessment schemes. Garmin encourages NIST to adopt the applicable language and provisions from ETSI EN 303 645 [303645] for conformity requirements. Similarly, consistency with ETSI TS 103 701 [103701] for assessment and documentation is likely to reduce the burden for global manufacturers and support mutual recognition schemes.

Clear and precise definitions of scope, both on the "consumer" and the "IoT" dimensions, are also needed for manufacturers, retailers, and end users to have a consistent understanding of the products and product categories that may be covered by a labeling scheme. Previous challenges in this area, as well as slightly varying definitions between [DCMS], [303645], the Consumer Product Safety Act (which defines Consumer Product), and other sources, are strong indications that this is an area of ambiguity. Garmin encourages NIST to select an existing, suitable definition given the goals of EO 14028, with consideration to the diversity of potential product categories and the associated diverse level of inherent risk. For example, a "rarely connected" device such as a fish-finder is inherently lower risk, as discussed in our position paper [GARMIN].

Comments on the Background and Methodology Section

The final paragraph of this section makes ambiguous use of the terms "profiles" and "baselines". "Profile of those baselines" could refer to profiles introduced in preceding paragraph: "these are core baselines and need to be tailored (or profiled) for specific use cases or sectors. This profiling...". Garmin proposes the alternative "Through a review of the landscape of related informative references from governments, nonprofit, and private sector sources, NIST developed **a unified super-set of baseline criteria (the "unified baseline")**. In selecting technical criteria for extending or editing *this unified baseline*, NIST applied the following considerations.

Comments on the Capabilities in Table 1

Asset Identification

While we appreciate that an asset identifier may facilitate asset management use cases, an identifier does not always directly improve security. In product categories where a consumer or household has only one of a device (e.g. a wearable, refrigerator, or home router), it is also less useful for securability.

Devices may be designed to work with multiple mobile apps or backend services. Likewise, the same mobile app and cloud service may be designed to work with multiple devices (as is the case for many Garmin wearable devices). In such cases, the device (rather than product) makes the most sense as the subject of identification (identified subject). Please change “IoT product” to “IoT device” under the Capability column, consistent with language used in NISTIR 8259A: "The **IoT device** can be uniquely identified…"

Inventory of components is a separate consideration from device identification. The Criteria column does not address criteria that would facilitate evaluation of conformance to the inventory concern. As such, we suggest striking 'and can inventory all the IoT product's components' from the description of the Capability.

For any physical identifier, accessibility to the consumer is the intended outcome; 'external or internal' is not necessary and may create confusion. Suggest striking this phrase from Criteria item 2.

The term "product component host" is used in this and other rows but is not defined. It is unclear whether this could refer to the main application processor in the IoT device, a companion mobile app, or other component such as a cloud service or gateway. Please add a definition according to intent; examples will also help clarify.

Product Configuration

For some product categories and use cases, physical access may need to be sufficient for authorization. For example, a home router may have a button that resets to factory settings, and a wearable may not require a password or PIN entry except for accessing the security-sensitive features (e.g. contactless payment). Any criteria or requirements associated with the Product Configuration capability should be restricted to cases where an authenticator (e.g. password or biometric) is used. Alternatively, add a note to clarify that physical possession of the device may implicitly authorize the bearer to restore/clear the product.

We would encourage a requirement for authentication, for any Product Configuration change that does not require physical access (e.g., occurs across the Internet or a wireless interface).

In the 3rd criterion, the "factory default" and "initialized" state[1] should be distinguished. Provisioning from the factory default state may require instructions or other parts of the IoT Product to have e.g. a knowable factory default password.

Data Protection

Depending on the product capabilities and business intent, confidentiality of the internal software may not be feasible or appropriate. Further, the integrity of the internal software is covered by the "Software Update" capability.

In cases where data is presented on the device without authentication (for usability or safety considerations), technical measures to protect confidentiality at rest add no value, and in fact may reduce the battery life of the device due to increased power consumption. For example, consider the case where the user takes a wearable or handheld on a weeklong hiking trip -- a forgotten password or PIN, or dead battery, could leave the user stranded and without a great way to navigate home. Allowable exceptions to the criteria need to account for such cases.

In the 3rd criterion, please strike "and any initial software included on the device (including updates)". The ability to render data inaccessible is useful for security, however the ability to render included software inaccessible is not.

These criteria are similar in intent to [303645] clauses 5.4, 5.5. and 5.8; Garmin encourages adopting these provisions as they provide clear and assessable language for stored and transmitted data.

Logical Access

Ability to disable access in an *unrecoverable* way should be excluded from the criteria and requirements. For example, if the product can only be configured using a USB port, disabling that USB port should not be required. Similarly, interfaces that are needed for maintenance (by any authorized party) or testing/refurbishment (upon return to the manufacturer) should not be disabled.

Logical Access is also covered by [303645] clause 5.1 and 5.6, and we encourage adopting the most relevant provisions as criteria.

Software Update

Cost or other constraints may mean that certain components of an IoT device are not updateable. Moreover, components may be intentionally non-updateable (immutable) by design for safety reasons. For these cases,

[1] See [303645], clause A.2 for a discussion of these states.

transparency and alternate plans are valuable. [ETSI] Provisions 5.3-14 and 5.3-15 allow for this alternative, and Garmin recommends allowing for this.

[303645] clauses 5.3 and 5.7 provide specific provisions with similar intent; Garmin recommends adopting the relevant subset.

Cybersecurity State Awareness

"Cybersecurity-related state information" is ambiguous, especially with regard to sufficiency. Any requirement should identify at least categories of information to record. However, as attack techniques evolve, new categories of state may become "cybersecurity related", and any given device may not have the capability to record such information. We would also suggest using the term "event logging" for consistency with SP800-53 control AU-2 [AU-2], or "telemetry data" for consistency with [303645].

Constrained devices may not have the storage capabilities to log information with reasonable retention.

This capability describes the product as able to "detect cybersecurity incidents", however the criteria only covers logging and access to the state information, not the processing needed to process the logged data to identify *unusual activity* or decide that the *unusual activity* is an *incident*. Detecting *incidents* may be challenging for an IoT device, be prone to false positives, and in the case of novel attacks, may require human insight (as indicated by [AU-6]).

Comments on the Capabilities in Table 2

Documentation

Criterion 1(e) may be challenging for larger and more complex products. As documentation this may be necessarily high level, with details only in the implementation of the source code and tests.

In criterion 1(h), "expected lifespan" and "term of support" should be restricted to security updates; other kinds of updates (e.g. addressing defects and improving performance) have no utility for security. [303645] makes this restriction via its definition of "defined support period".

Criterion 4 should be phrased to allow for individual criteria or requirements to be not applicable.

In footnote 3 to criterion 5(b), we suggest striking "application development" from the description of IoT Platform; while the platform provider may provide integrations such as a software development kit to support development and integration, this is not an operational capability. Since other platforms and tools are likely to be used in application development this is also confusing.

Footnote 3 also seems to contemplate the documentation being available to the user ("allow for the IoT user to more accurately determine risks"). However, the "Documentation" capability itself does not indicate that any of the information is to be published. **Many of the criteria in this section may contain confidential and proprietary information that conveys a business advantage**; as such we caution against requiring disclosure of more information than is necessary for the consumer to make a purchase/use decision.

Information and Query Reception

As general bug reports may be less sensitive than vulnerability reports, and these criteria are focused on security, "maintenance and" as well as the example of "bug reporting capabilities" should be struck from criterion 1.

Information Dissemination

In criterion 1(a), replace "software updates" with "security updates" as other kinds of updates are not in scope for this profile, and a manufacturer or supporting entity may choose to have different terms of support for security vs. other updates.

We believe criterion 2 (alerting ecosystem entities) does not necessarily improve security for *consumers*; further some of the information listed may be considered confidential and proprietary.

Education and Awareness

In criterion 4, the duration and scope of security updates may not be appropriate for product packaging as this is a fixed medium. A manufacturer is disadvantaged if they choose to extend the support period, and the product packaging may be unavailable for purchases made online. Garmin encourages NIST to adopt the language of [303645] Provision 5.3-13: "The manufacturer shall publish, ***in an accessible way that is clear and transparent to the user***, the defined support period."

Comments on the Capabilities in Table 3

The Additional Criteria in Table 3 appear to be either unnecessary, not broadly feasible, or in some cases may harm security.

For example:

- Product Configuration item 1: Ability to change other components' configuration may provide a means for an attacker to pivot through the components in a product.
- Logical Access item 1(b): Validating data sent is usually unnecessary as the component should be designed to generate well-formed data, and additional validation may impact performance or battery life.
- Software Update item 1(a): Authenticating an update on behalf of another component introduces a CWE-367 (Time Of Check/Time Of Use) weakness if the communication between components can be tampered with.
- Product Security item 1: The Data Protection criteria in table 1 are sufficient to ensure connections are secure; the reestablishment following an outage is more of a functionality concern than one of security.

References

[AU-2] NIST. "SP 800-53 Rev 5.1 and SP 800-53B: AU-2 Event Logging" https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control?version=5.1&number=AU-2. Accessed Oct 15. 2021.

[AU-6] NIST. "SP 800-53 Rev 5.1 and SP 800-53B: AU-6 Audit Record Review, Analysis, and Reporting" https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control?version=5.1&number=AU-6. Accessed Oct 15. 2021.

[CPSA] Consumer Product Safety Act, 15 U.S.C 2051-2089. https://www.cpsc.gov/PageFiles/105435/cpsa.pdf Accessed Oct 14, 2021.

[DCMS] UK DCMS "Government response to the call for views on consumer connected product cyber security legislation". Policy Paper. GOV.UK, April 21, 2021. https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation Accessed Oct 14, 2021.

[GARMIN] Garmin International "NIST position paper on Consumer IoT labeling". Position Paper. August 17, 2021. https://www.nist.gov/system/files/documents/2021/09/03/Garmin-NIST-position-consumer-IoT-labeling.pdf. Accessed Oct 15, 2021.

[103701] ETSI. Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements. TS 103 701 v 1.1.1. August, 2021. https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf Accessed Oct 14, 2021.

[303645] ETSI. Cyber Security for Consumer Internet of Things: Baseline Requirements. EN 303 645 v 2.1.1. June, 2020. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf Acces sed Oct 14, 2021.