Answer to: DRAFT Baseline Criteria for Consumer Software Cybersecurity Labeling

Submitted electronically to: labelingeo@nist.gov

Dear NIST cybersecurity team,

TÜV SÜD is pleased to contribute to public consultations NIST is organizing on cybersecurity topics.

About TÜV SÜD: we are a third-party laboratory with experience on labelling for consumer IoT products with projects on going or completed with Finland Trafficom label, Singapore CLS label, TÜV SÜD own label CSC.

Our review of the document and our suggestions are informed by our experience of providing testing, certification and labelling for a wide area of products on different schemes, worldwide.

Sincerely,

Maxime Hernandez

Senior Engineer

TÜV SÜD

1. **Whether criteria will achieve the goals of the EO by increasing consumer awareness and information and will help to improve the cybersecurity of software which they purchase and use.**
   Response:
   It will help to achieve the goal (In order to improve any issue it is necessary to make it visible – which a label can do) but the full success will depend on its implementation.

2. **Whether the criteria will enable and encourage software providers to improve the cybersecurity aspects of their products and the information they make available to consumers.**
   Response:
   Yes. Even the label are not mandatory it will be seen as a competitive advantage by proving additional information to the buyer. Several studies on the topic quoted that information about a product security will influence a buying decision criteria.

3. **Whether the labeling-specific criteria are appropriate and likely to be effective for consumers.**
   Response:
   Overall yes. In details, the "Free from Hard-Coded Secrets" might confuse a buyer not familiar with this topic. Moreover the "*Personally Identifiable Information (PII) Data Manifest*" seems incomplete and might mislead buyers.

4. **Whether a single, overarching statement that the software product meets the NIST baseline technical criteria should be included on a label, or whether alternative statements would be appropriate.**
   Response:
   The issue with meeting a "NIST baseline" is that if it is linked in the name to a government agency, buyers might think it is totally secure. Remarks would be to 1) Mentioning "NIST" (as a government agency) will increase market acceptance and consumer trust in the label 2)There should be in the immediate surrounding of the sentence a detailed explanation of what this baseline is and stating it doesn't mean the product is 100% secure. 3) Clarify that NIST endorsement is for the scheme not the product.

5. **Whether additional considerations for the labeling approach, consumer education, or testing are needed – including:**
   a. **Possible appropriate definitive text for describing the labeling program in consumer education materials**
   b. **Best approaches for addressing the needs of non-English speaking consumers**

   Response:

Regarding b): product should have a QR that scan be scanned and go to a URL where the user can select the language. Icons can also be used (in this case the icon should be standardized to avoid misunderstanding).

6. **Whether the software label approach and design should be unique or extended to the IoT product label (also directed in the EO) to facilitate brand recognition, even though the technical criteria will be different.**
   Response:
   It makes sense to have a global approach on these topics.

7. **Whether the conformity assessment provisions are appropriate.**
   Response:
   Yes. assessment provisions are appropriate. Additionally, in the early stage, to ensure trust, quality, consistency in the new scheme audits shall be perform by entity compliant with standards such as ISO 17025 for testing.

8. **Whether a template Declaration of Conformity would be useful for software providers.**
   Response:
   Yes, template is definitely useful. Without guidance manufacturer will not know what to use.

9. **Whether more details on evidence required to support assertions would be useful for software providers.**
   Response:
   It will be useful and there will be a need for a specific guidance document.

10. **Whether the technical baseline criteria are appropriate, including but not limited to:**
    a. **The feasibility, clarity, completeness, and appropriateness of attestations**
    b. **Normative references to be considered for inclusion**
    c. **Potentially requiring that the Software Identifiers attestation take the form of a Software ID Tags**

    Response:

    See details below on each criteria:

2.3.1.1 *Software Provider*

Attestation	Software Provider
Description	Information relating to the entity that is making attestations in the label.
Desired Outcome	Consumers can quickly and easily determine the author/organization of the software that is making claims.
Assertions	The name of the software developer/vendor/owner making the claims in the label as well as the name and contact information for an individual within this entity that is responsible for these claims is readily available to the consumer.

➔ The Description exclude de-facto third party lab independent assessment to be mentioned in the label. But this possibility is listed in "Conformity Assessment Criteria" "The software provider has the option of using an accredited laboratory or inspection body, which would be indicated on the declaration". It makes sense for the consumer to be able to identify easily if the service provider has worked alone or was checked by an external entity. Suggestion is that this information can be displayed on the label.

2.3.1.2 *Label Scope*

Attestation	Label Scope *Note: Any reference to "software" in the attestations below should be understood to mean "software within the label scope."*
Description	A clear description of all software systems under the purview of the label that is readily understandable by the consumer. All other software required for the software to function but is outside the purview of the label should be described.
Desired Outcome	Consumers clearly understand what the attestations conferred by the label apply to. For example, if the attestations made in the label are only applicable to a mobile application running on a consumer's mobile device, the Label Scope description should make this clear. This will enable consumers to better understand security attestations made about the software as well as allow the consumer to better compare the characteristics of varying software products.
Assertions	The software provider attests to the completeness and correctness of the provided software description and this information is readily available to the consumer.

➔ Need to clarify in "Description" what is a "clear description" : is it a software image? A list of sub-partionning? Or a list of functions supported by the software that are available to the user? Or re-use the 2.3.13 software identifiers?

2.3.1.3 Software Identifiers

Attestation	Software Identifiers
Description	A standardized, unique identifier for each piece of software
Desired Outcome	Consumers can clearly understand version/build/editions and any other key identifying characteristics to which a label refers. Likewise, consumers can use an identifier to determine if a piece of software is bound to a label.
Assertions	The software provider attests to the completeness and correctness of the software identifiers and this information is readily available to the consumer.

Between the time of the label validation and the time the product will be in the store there is likely to have software change. How will the buyer be informed about the potential gap?

2.3.1.5 Software End of Support Date

Attestation	Software End of Support Date
Description	A date beyond which the consumer can expect to no longer receive security-related updates for any software within the Label Scope.
Desired Outcome	The consumer should clearly understand how long they can expect the software to be maintained and updated to remediate security vulnerabilities.
Assertions	The software provider asserts the software will continue to receive security-related updates until at least the date specified.

In the “assertion” there is “until **at least** the date specified” which seems to contradict the “attestation” “Software **end of** Support”. Suggestion to rename the attestation to “Minimal duration of support”

2.3.1.6 Vulnerability Reporting

Attestation	Vulnerability Reporting
Description	The mechanism by which consumers can determine if a vulnerability for the software has been identified by the organization.
Desired Outcome	The consumer should be confident the developer can respond to vulnerabilities discovered in their software. Furthermore, consumers should be confident that developers reasonably report vulnerabilities to affected parties.
Assertions	The software provider asserts to reporting vulnerabilities to consumers in a reasonable mechanism either through hosting vulnerability information internally and/or reporting vulnerabilities to the National Vulnerability Database [NVD] or other appropriate vulnerability repository. The software provider makes it clear how to obtain this information [VDP].

In Desired Outcome "can **respond** to vulnerabilities" : the word "respond" would mean to patch a vulnerability but in the Description there is "if a vulnerability for the software has been **identified** ". "Identified" and "Respond" does not seems to have the same meaning. Suggestion: delete the sentence "The consumer should be confident the developer can respond to vulnerabilities discovered in their software "

2.3.3 Critical Cybersecurity Attributes and Capability Attestations

2.3.3.1 Free from Known Vulnerabilities

Attestation	Free from Known Vulnerabilities
Description	The provider attests that known vulnerabilities have been fixed.
Desired Outcome	Consumers should be confident when selecting software that it is free from known vulnerabilities.
Assertions	The software provider asserts in good faith that as of the assertion date indicated in the label, the software is free from known vulnerabilities.

- ➔ There will be a time difference between the label printing and the consumer buys the product in the store. What insurance the buyer will receive for this period that the device has been updated or not?
- ➔ Additionally, not all vulnerability need to be patched. It depends on the risk and severity of the vulnerability.

2.3.4 Data Inventory and Protection Attestations

2.3.4.1 Personally Identifiable Information (PII) Data Manifest

Attestation	Personally Identifiable Information (PII) Data Manifest
Description	Personally Identifiable Information Data is data that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. The label addresses whether common types of PII data are either stored, processed, or transmitted by the software and how that data is safeguarded.
Desired Outcome	Consumers should clearly understand what PII the software stores, processes, or transmits and how that data is safeguarded.
Assertions	The software provider makes one of the following assertions: • **Supports** – The software provider states if the software accesses any of the types of PII listed below. Furthermore, it specifies if this data is encrypted when stored or transmitted and if this is done by the software itself or externally. This information is made available to the consumer. o Social security numbers, passport numbers or any similar official ID number o Banking, financial, or medical account numbers o Medical information **Not Applicable** – The software does not store, process, or transmit any PII data.

➔ The list of PII seems shorts. Suggestion: provide a quote from a legal USA framework for the list of PII.

2.3.4.2 Location Data Manifest

Attestation	Location Data Manifest
Description	Location Data is any data that is stored, processed, or transmitted by the software that can be used to determine the location of a system running the software. The Location Data Manifest should contain all Location Data and how that data is safeguarded.
Desired Outcome	Consumers should understand exactly what Location Data is stored, processed, or transmitted by the software and how that data is safeguarded.
Assertions	• **Supports** – The software provider maintains a full manifest of all Location Data and how the provider safeguards that data and makes that information available to the consumer. The software provider also describes how precise the location data used by the software is • **Not Applicable** – The software does not store, process, or transmit any Location Data.

-> In "Assertion" it seems the end of the sentence is missing.