Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Microsoft

December 16, 2021

Submitted via email to labeling-eo@nist.gov.

National Institute of Standards and Technology (NIST)
United States Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20889

Re: NIST's Draft Criteria for Consumer Software Cybersecurity Labeling

Microsoft appreciates the opportunity to provide feedback on NIST's *Draft Criteria for Consumer Software Cybersecurity Labeling*. We are supportive of a voluntary pilot program to understand the benefits, costs, and impacts of a consumer software cybersecurity labeling program, and we encourage NIST to focus on outcome- and risk-centric criteria as part of that program.

Addressing NIST's direct questions to reviewers:

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.

The criteria have the potential to help achieve the goals of Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, and to enhance the cybersecurity of software that consumers purchase and use; however, further study is needed. Research into prior voluntary labeling efforts may provide insight into supplier behavior (e.g., do labeled products have higher quality than unlabeled products?), consumer behavior (e.g., do consumers choose higher quality products?), and outcomes (e.g., does the quality measure reflect the desired outcome?). Likewise, we believe that a pilot program as envisioned by the EO could provide real-world insight into the benefits, costs, and broader impacts of a labeling program.

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.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Microsoft

Software providers leverage or reference a myriad of national and international standards, industry recommendations, regulatory and procurement requirements, and internal policies. The World Economic Forum lists "Fragmented and complex regulations" as a leading cybersecurity challenge of 2021,[1] saying: "Individual regulations may have similar intent, but multiple policies add complexity for businesses that need to comply with all regulations."

Instead of defining new baseline criteria for consumer software cybersecurity labeling, these criteria should be incorporated into or draw from NIST SP 800-218 (Draft), and the process for obtaining a label should require attesting to following NIST SP 800-218 (Draft) or to a defined list of practices or tasks from it.

Using consistent baseline criteria across multiple programs (such as consumer software labeling and EO 14028) enables software providers to implement and attest to or demonstrate conformance to the baseline criteria once. This will lead to more consistent and streamlined implementation of those baseline criteria because cybersecurity resources can be focused on fewer overlapping or conflicting criteria.

Incentivizing software providers – for example, by providing safe harbors from other regulations for consumer software that conforms with the label – may increase adoption of the voluntary label and further the outcomes it aims to achieve. Microsoft discusses this approach in more detail in *Microsoft proposes incentivizing digital solutions to mitigate supply chain risk.*[2]

Whether the labeling-specific criteria are appropriate and likely to be effective for consumers.

The proposed criteria are too implementation-specific and detailed to effectively communicate to the diverse consumer software demographic. Consumers should be presented with outcome- or risk-centric statements about the software, such as:

- Built using secure development practices.
- Supports automatic updates.
- Protects stored and transmitted information.

[1] https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/
[2] https://blogs.microsoft.com/on-the-issues/2021/03/23/incentivizing-digital-solutions-mitigate-supply-chain-risk/

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Microsoft

- Handles sensitive information.

This model would be consistent with the Content Descriptors used for TV[3] and video game[4] ratings.

Similarly, focusing on outcomes and providing implementation examples, rather than prescribing implementations, will afford software providers flexibility to tailor implementations to the technologies and platforms they use and their consumers' needs. This approach will also future proof the label's criteria against emerging or changing technologies.

The criteria should be risk-based and take into consideration the platform that the consumer software is deployed on. For example, the typical consumer will not be able to, nor should they need to, understand the difference between strong cryptography provided by the platform and strong cryptography implemented by the consumer software; their desired outcome is that consumer software that handles sensitive information protects it.

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.

Microsoft appreciates the context provided in *Appendix A: Additional Context for Labeling Criteria* and agrees with NIST's conclusion that a "binary label with a layered approach" would be appropriate for a consumer software cybersecurity label. The complex interconnected nature of modern software and the need to update information – especially for software that is supported for many years – reinforces the approach of a minimal binary label from which you can access a website with more detailed and up-to-date information. As NIST has identified, this website can also provide contextual information about relevant criteria to improve consumer education. The label itself may benefit from including a small number of outcome- or risk-centric statements as Content Descriptors, as discussed in the previous answer, to call consumers' attention to specific criteria.

[3] http://tvguidelines.org/ratings.html
[4] https://www.esrb.org/ratings/

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Whether additional considerations for the labeling approach, consumer education, or testing are needed.

We have no additional considerations beyond those discussed elsewhere in this response or that would be learned through the pilot program.

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.

IoT devices will always have a software component, whether it is on the device itself, or software used to interact with or manage the device. Based on this assumption, the IoT label should be an extension of the consumer software label and add IoT-specific criteria to the consumer software criteria.

Whether the conformity assessment provisions are appropriate.

Consumer software has been trending to update more frequently – with time between updates being measured in days or weeks instead of months or years. A Supplier's Declaration of Conformity (SDOC) is an appropriate method of conformity assessment to achieve transparency and maintain agility.

Consumer software providers range from Fortune 500 companies to hobbyists and are based around the globe; using an SDOC ensures a low barrier to enter the consumer software ecosystem and avoids disproportionately affecting smaller software providers or providers of low-cost or free consumer software.

Whether a template Declaration of Conformity would be useful for software providers.

Since templates drive consistency, they are typically beneficial to both software providers and consumers. Any variable information in the template (i.e., information that is software provider or software specific) should be clearly delineated to help consumers identify specific vs generic content and to help software providers identify content they are responsible for providing.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Microsoft

Whether more details on evidence required to support assertions would be useful for software providers.

NIST SP 800-218 (Draft) identifies "Implementation Examples" rather than prescribing specific implementations to afford software providers flexibility to choose specific implementations based on their business or technical needs and to insulate NIST SP 800-218 (Draft) against emerging and changing technologies and techniques. For this same reason, we recommend that the required evidence is not prescriptive but instead describes features of the evidence and provides examples.

Whether the technical baseline criteria are appropriate, including but not limited to:

The feasibility, clarity, completeness, and appropriateness of attestations

2.3.1.1 Software Provider

We recommend that individuals' names and contact information are not made publicly available because they tend to change frequently and to minimize disclosure of PII (Personally Identifiable Information) and potential risks to those individuals. Instead, we recommend providing a contact website address.

2.3.1.3 Software Identifiers

We address this in more detail in *Potentially requiring that the Software Identifiers attestation take the form of a Software ID Tags* below. In addition to machine-readable software identifiers, the software provider should be able to provide a human-friendly software identifier.

2.3.1.5 Software End of Support Date

Software licenses for free and open source software often disclaim any ongoing support obligation. Effort should be made to not penalize this software while still supporting customer awareness.

2.3.2.1 Implements a Secure Development Process

Consumers should be made aware that a secure development process reduces risk but does not eliminate it entirely.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Microsoft

2.3.3.1 Free from Known Vulnerabilities

This criterion has a few issues:

1. Vulnerabilities are often found after the software is released; therefore, a point-in-time declaration of software being free from known vulnerabilities – especially when that declaration is made before the software is released – risks giving consumers a false sense of security.
2. NIST SP 800-218 (Draft) already includes practices and tasks to find, triage, and remediate vulnerabilities (PW.7, PW.8, and RV). Therefore, this criterion is already covered by the "Implements a Secure Development Process" criterion.
3. NIST SP 800-218 (Draft) RV 2.2 acknowledges making risk-based decisions about whether to remediate vulnerabilities or to address the risk through other means. Requiring attestation of software being free of known vulnerabilities undermines being able to make risk-based decisions.
4. It could disincentivize looking for vulnerabilities because there would be an obligation to immediately fix them.

We encourage NIST to remove this criterion and focus on criteria that reduce the probability of vulnerabilities being introduced (e.g., "Implements a Secure Development Process"); encourage coordinated vulnerability disclosure, triage, and remediation of vulnerabilities by software providers; and encourage installation of software updates by consumers.

2.3.3.3 Multifactor Authentication

It is important to scope this criterion so consumers have context to seek multifactor authentication where it would be especially beneficial (i.e., consumer software that stores sensitive information or can be accessed remotely).

2.3.3.4 Free from Hard-Coded Secrets

This criterion should be included in NIST SP 800-218 (Draft) and incorporated into the "Implements a Secure Development Process" criterion.

2.3.3.5 Strong Cryptography

This criterion should be pivoted to focus on the desired outcome, the protection of sensitive information in transit and at rest. The consumer should not have to be concerned whether that is provided by the software or by the platform running the

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Microsoft

software. This criterion is also covered in NIST SP 800-218 (Draft) and therefore by the "Implements a Secure Development Process" criterion. It may improve conformance and consumer attention if this criterion is only emphasized for consumer software that handles sensitive information.

2.3.4 Data Inventory and Protection Attestations

These criteria could better communicate risk to consumers by focusing on local storage vs remote transmission:

1. Does the software store sensitive information? If so, what does it store?
2. Does this information transmit sensitive information? If so, what does it transmit?

The software provider should, optionally, be able to provide a website address for a privacy policy.

A consumer may also want to know if core functionality provided by the software requires remote services from the software provider to operate. For example, a consumer may prefer to purchase an IoT garage door opener that can operate without remote services.

Normative references to be considered for inclusion

We recommend that most of the criteria reference practices or tasks in NIST SP 800-218 (Draft) and that any criteria not included in NIST SP 800-218 (Draft) be considered for inclusion. To avoid ambiguity for software providers and consumers, we recommend against multiple normative references.

Potentially requiring that the Software Identifiers attestation take the form of a Software ID Tags

Software identification is complex and will evolve with the increased production and exchange of software bills of materials (SBOMs). Multiple software identification schemes are already in use across the industry: Software ID Tags (SWID)[5], Concise Software Identification Tags (CoSWID)[6] (an alternate

[5] https://www.iso.org/standard/65666.html
[6] https://datatracker.ietf.org/doc/draft-ietf-sacm-coswid/

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Microsoft

representation for SWID Tags), Common Platform Enumeration (CPE)[7], SoftWare Heritage persistent IDentifiers (SWHIDs)[8], package URL (purl)[9], and more.

We recommend that software providers be able to associate multiple software identifiers from multiple schemes with a consumer software label, and that the list of schemes be easily extendable in the future as new schemes evolve. This will allow software providers to disclose all known software identifiers for their software, which will improve the ability to correlate other information about the software (such as known vulnerabilities).

Microsoft remains committed to our ongoing partnership with NIST, and we welcome future opportunities to collaborate.

Respectfully submitted,

William Bartholomew
Principal Security Strategist, Global Cybersecurity Policy
Digital Diplomacy
Microsoft Corporation

[7] https://nvd.nist.gov/products/cpe
[8] https://docs.softwareheritage.org/devel/swh-model/persistent-identifiers.html
[9] https://github.com/package-url/purl-spec