

Recommended Criteria for Cybersecurity Labeling of Consumer Software

National Institute of Standards and Technology

February 4, 2022

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.CSWP.02042022-1>

Abstract

Executive Order (EO) 14028, “Improving the Nation’s Cybersecurity,” tasks the National Institute of Standards and Technology (NIST), in coordination with the Federal Trade Commission (FTC) and other agencies, to initiate pilot programs for cybersecurity labeling. These labeling programs are intended to educate the public on the security capabilities of ...software development practices. To inform this effort, the EO directs NIST to “...**identify secure software development practices or criteria for a consumer software labeling program....**” This document seeks to fulfill this directive by making recommendations in the following areas: 1) the role of a scheme owner in a labeling program, 2) baseline technical criteria that can inform a label, 3) labeling presentation criteria, and 4) conformity assessment criteria. This document also explores consumer education and usability for software labels.

Keywords

consumer software; criteria; cybersecurity; executive order; label.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST, nor does it imply that the products mentioned are necessarily the best available for the purpose.

Additional Information

For additional information on NIST’s Cybersecurity programs, projects and publications, visit the [Computer Security Resource Center](#). Information on other efforts at [NIST](#) and in the [Information Technology Laboratory](#) (ITL) is also available.

Submit comments on this publication to: labeling-eo@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

All comments are subject to release under the Freedom of Information Act (FOIA).

Acknowledgments

The authors of this document wish to thank all of those who provided input on this effort—especially those who attended our workshops, participated in one-on-one phone calls, and provided written comments on our draft.

Audience

This document is intended for three primary audiences:

1. Organizations which may be interested in implementing a labeling scheme for consumer software.
2. Organizations which produce or distribute consumer software and are interested in participating in future labeling programs.
3. Consumers who are interested in understanding a potential future labeling program.

Document Conventions

The terms “should” and “should not” indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited.

Table of Contents

1	Introduction	1
1.1	Background.....	1
1.2	Document Scope and Goals	1
1.3	Labeling Schemes and Scheme Owners	2
1.4	Document Structure	3
2	Baseline Technical Criteria for Consumer Software Labels	4
2.1	Methodology	4
2.2	Recommended Criteria	5
3	Labeling Criteria.....	16
3.1	Binary Label.....	16
3.2	Layered Approach.....	17
4	Conformity Assessment Criteria	18
References	19	

List of Appendices

Appendix A— Additional Context for Labeling Criteria	23	
A.1	Introduction	23
A.2	Methodology	23
A.3	Labeling Approaches	24
A.3.1	Label Types.....	24
A.3.2	Recommended Label Approach	25
A.3.3	Label Presentation.....	26
A.3.4	Addressing Potential Weaknesses	27
A.4	Consumer Education	27
A.5	Consumer Usability and Testing	29
A.5.5	Usability Considerations	29
A.5.6	Consumer Testing	31
Appendix B— Abbreviated SSDF Example	33	

1 Introduction

1.1 Background

This document provides recommended criteria for a cybersecurity labeling effort for consumer software practices. Executive Order (EO) 14028, “Improving the Nation’s Cybersecurity,” issued on May 12, 2021, directed the National Institute of Standards and Technology (NIST) to develop these criteria in coordination with the Federal Trade Commission (FTC) and other agencies for use in a pilot program¹. NIST is identifying key elements of a potential labeling program which could be established by another organization. The criteria that NIST is recommending are stated in terms of minimum requirements and desirable attributes; NIST is not establishing its own program. Aspects of a pilot program are described in a separate document.

NIST was directed to “...identify secure software development practices or criteria for a consumer software labeling program....” to “reflect a baseline level of security practices, and if practicable... increasingly comprehensive levels of testing and assessment that a product may have undergone.”

NIST also was directed to “examine all relevant information, labeling, and incentive programs, employ best practices, and identify, modify, or develop a recommended label or, if practicable, a tiered software security rating system.” This review “shall focus on ease of use for consumers and a determination of what measures can be taken to maximize participation.” This document addresses these tasks.

1.2 Document Scope and Goals

Software is an integral part of life for the modern consumer. Nevertheless, most consumers take for granted and are unaware of the software upon which many products and services rely. From the consumer’s perspective, the very notion of what constitutes software may even be unclear. While enabling many benefits to consumers, that software – that is, software normally used for personal, family, or household purposes – can also have cybersecurity flaws or vulnerabilities which can directly affect safety, property, and productivity.

There is no one-size-fits-all definition for cybersecurity that can be applied to all types of consumer software. The [risk](#) associated with software is tightly bound to that software’s intended use (both in function and operating environment), as well as its post deployment configuration. The cybersecurity considerations appropriate for a mobile game will differ from those applied to an online banking app or to run the media station on an automobile.

This document addresses the need to develop appropriate cybersecurity criteria for consumer software. It also informs the development and use of a label for consumer software. This in turn can improve consumers’ ability to take cybersecurity into account when making decisions about software selection and use. The following key recommendations are addressed:

¹ For more information, see sections 4(s) and 4(u) of Executive Order 14028 [[EO14028](#)]

- Establish a baseline set of technical criteria to help organizations wishing to make claims about security via a software label. These convey to the consumer that good practices for secure software development were employed during the lifecycle of the software and that security-related software architecture, functionality, and other attributes follow baseline technical criteria.
- Provide criteria for the label including:
 - How cybersecurity-related risks and attributes could be represented
 - How labels can be tested for effectiveness
 - How the public can be educated about the label and its meaning
- Describe conformity criteria for use by organizations

It is important to stress that these criteria define a baseline of due diligence related to the cybersecurity and related labeling of consumer software products. They are intended to increase purchasers' and users' awareness and information about consumer software cybersecurity. They also aim to avoid overconfidence in the level and type of cybersecurity related to the software at a particular point in time.

These criteria identify key elements of labeling programs in terms of minimum recommendations and desirable attributes.

This document is **not** intended to describe how a cybersecurity label should be explicitly represented (either physically or digitally) – nor is it intended to detail how a labeling program should be owned or operated.

NIST is not designing a particular label – nor is NIST establishing its own labeling scheme for consumer software. Rather, these criteria set out desired outcomes, allowing and enabling the marketplace of providers and consumers to make informed choices.

These criteria are intended to complement and not to conflict with the [IoT Product Criteria](#) which meet the goals of [Sec. 4 \(t\)](#) of Executive Order 14028 [[EO14028](#)]

1.3 Labeling Schemes and Scheme Owners

A label indicates to consumers that software has been demonstrated to meet specified requirements. Software becomes labeled through a labeling scheme. **The scheme owner is the entity that manages the labeling scheme and determines its structure and management and performs oversight to ensure that the scheme is functioning consistently with overall objectives.** Scheme owners can be public or private sector organizations.

A labeling scheme provides answers to the following questions:

1. What are the requirements for getting a label?
2. What does the label look like and what information should it contain?
3. What is the process for obtaining and displaying a label on software?

The following sections of this document make recommendations concerning criteria for answering these questions. However, many of the requirements needed to fulfil the recommended criteria

will need to be established by the scheme owner. The goal of this document is to provide recommendations, additional information, and context related to these responsibilities for use by a scheme owner creating the consumer software labeling program.

As previously mentioned, there is no one-size-fits-all definition for cybersecurity that can be applied to all types of consumer software. To achieve the outcomes described in the baseline criteria, the scheme owner will need to adapt and refine scheme requirements that meet the needs of the software seeking labels.

1.4 Document Structure

The remainder of this document is organized as follows:

- [Section 2](#) – contains the baseline technical criteria for the label and methodology used to arrive at those criteria
- [Section 3](#) – describes criteria for the labeling approach and consumer-focused label information
- [Section 4](#) – describes conformity assessment and proposes multiple approaches for a labeling scheme
- [Appendix A](#) – provides additional details on labeling criteria and considerations, including labeling approaches, consumer education, usability, and consumer testing
- [Appendix B](#) – contains an abbreviated excerpt from the Secure Software Development Framework

2 Baseline Technical Criteria for Consumer Software Labels

2.1 Methodology

2.1.1 Overview

This section describes the technical criteria as a series of *claims* about the software. For each claim, there is both a description and a statement about what the reader of the label should be able to learn related to that claim. When referenced by the label, the consumer is informed about these *outcome-based* assertions and associated information. Additional information about conformity assessment related to consumer software labeling appears in [Section 4](#).

The claims are organized into three categories:

1. **Descriptive Claims** – This category describes information about the label itself. It grounds the label by identifying who is making claims about information within the label, what the label applies to, when the claims were made, and how a consumer can obtain other supporting information required by the label.
2. **Secure Software Development Claims** – This category describes how the software provider claims to adhere to accepted secure software development practices throughout the software development lifecycle. By addressing these criteria, the label communicates to the consumer that secure software development best practices were employed.

This section only specifies criteria in terms of what information should be made available to the consumer. It **does not** specify how these should be represented within the label itself. Label representation criteria are addressed in later sections of this document.

2.1.2 Terminology Conventions

The Descriptive Claims group defines two terms, **Claimant** and **Label Scope**:

A **Claimant** is defined in broad terms to encompass organizations of varying sizes and functions. This allows for individual developers, developer organizations, publishers, and others to act as the entity making the claims represented in a label and allows for flexibility on the part of the scheme owner.

The **Label Scope** refers to what a label is describing. This allows a claimant to distinguish among software that is either included or excluded from the claims backed by the label (e.g., a mobile app versus a back-end server). This is especially important to the consumer, as it is often difficult to determine where these systems begin and end – their boundaries. For brevity, the criteria in this document frequently use the term “software” and should be understood as referring to “software within the label scope.”

2.1.3 The Secure Software Development Framework

The core goal of this section is to establish secure development criteria appropriate for labels. There are many security development practices that are widely used. Rather than attempt to prescribe an exhaustive list of the competing standards and guidance in this space, the criteria in

this section make extensive reference to the NIST Secure Software Development Framework (SSDF)[[SSDF](#)].

The SSDF identifies common practices that are components to a secure software development process, and organizes them into four groups:

- Prepare the Organization (PO)
- Protect the Software (PS)
- Produce Well-Secured Software (PW)
- Respond to Vulnerabilities (RV)

The practices in each group are subdivided into related tasks. For each task, the SSDF references existing secure development practices documentation. See [Table 2](#) in Appendix B for an example practice/task.

The recommended consumer software labeling criteria leverage the SSDF in two ways. First, the claim “*Implements a Secure Development Framework*” references the SSDF in its entirety. It conveys that the scheme owner will be responsible for identifying and tailoring the SSDF’s practices to match the needs of its environment. This gives the scheme owner the flexibility of selecting appropriate tasks from the SSDF and to identify secure development practices already being instrumented by software developers in the relevant community.

The second way this document references the SSDF is found in the “*Minimum Secure Development Claims*” category. Where possible, the claims in this category reference explicit tasks in the SSDF. The claims made in this section are recommended to be included in all schemes.

2.2 Recommended Criteria

This section describes the recommended criteria. **To label consumer software, it is recommended the scheme owner require claimants to address all criteria at a minimum.** For each claim, this document defines the following attributes:

- Claim – A short title for the claim
- Description – A statement about what information the claim should capture
- Desired Outcome – The outcome and/or reasoning for including the claim in the label focusing on how this benefits the user of the label.
- Assertions – Factual statements made by the claimant that are conveyed with the claim.

A summary of each category and the names of each of the claims appear below:

- **Descriptive Claims**
 - *Claimant*
 - *Label Scope*
 - *Software Identifiers*
 - *Claim Date*
 - *Security Update Status*

- *Minimum Duration of Security Update Support*
- *Security Update Method*
- **Secure Software Development Claims**
 - *Implements A Secure Software Development Process*
 - *Practices Secure Design and Vulnerability Remediation*
 - *Practices Responsible Vulnerability Reporting Disclosure*
 - *Uses Multifactor Authentication (if applicable)*
 - *Free from Hard Coded Secrets*
 - *Uses Strong Cryptography (if applicable)*
 - *User Data is Identified and Secured*

The remainder of this section provides detailed descriptions for each of these claims.

2.2.1 Descriptive Claims

2.2.1.1 Claimant

Claim	Claimant
Description	Information relating to the entity that is making claims in the label. This entity is responsible for attesting to the completeness, correctness, and accuracy of all other claims made in the label. This entity could be the software developer or a third party who has been granted the authority to make such claims by the labeling scheme owner
Desired Outcome	Consumers can quickly and easily determine the entity making the claims contained within or conveyed by the label. It is crucial that consumers not misattribute claims made within the label to retailers, vendors, publishers, etc. when selecting software.
Assertions	<p>The claimant provides and asserts to the accuracy of identifying and/or contact information required by the labeling scheme owner and this information is made readily available to the consumer. This information may include, but it not limited to:</p> <ul style="list-style-type: none">• Claimant name• Claimant email address• Claimant mailing address• Claimant website

This contact information should correspond to the entity responsible for the claims in the label.

The information provided conforms to the requirements of the scheme owner.

2.2.1.2 Label Scope

Claim	Label Scope
<p>Note: Any reference to “software” in the attestations below should be understood to mean “software within the label scope.”</p>	
Description	A clear description of all software systems subject to the claims in the label. Any software system that provides significant or critical functionality for the labeled software but is not included in the label’s claims should be described.
<p>Note: the form and format of this description should be crafted by the label scheme owner to meet the needs of various types of consumer software.</p>	
Desired Outcome	<p>Consumers clearly understand what the claims conferred by the label apply to and can use this information when selecting consumer software.</p> <p>The boundaries that define software are often obscure to consumers. What may be perceived as a singular software product may contain multiple components, be distributed across different systems, or be owned by multiple organizations. Likewise, claimants may not have the authority or ability to make claims about all these various systems.</p> <p>For example, if the claims made in the label are only applicable to a mobile application running on a consumer’s mobile device and not the back-end system the application communicates with, the label scope should make this clear.</p>
Assertions	<p>The claimant attests to the completeness, correctness, and relevance of the provided information. This information is readily available to the consumer.</p> <p>The format and content of the information adheres to the requirements of the scheme owner.</p>

2.2.1.3 Label-Software Link

Claim	Label-Software Link
Description	A formalized mechanism that can be used to associate a label with the software described in the label scope
<p>Software is constantly being updated and modified. Likewise, a label may need to be amended, updated, or revoked. Elapsed time between the publishing of a label (especially regarding labels printed on physical packaging) and receipt by the consumer may cause confusion concerning the status of the label’s claims.</p>	

Conversely, organizations involved in the creation and distribution of software will likely desire to trace claims from a label to specific pieces of software for liability reasons

The scheme owner should require a standardized binding mechanism to couple the claims in each label to specific software. The label scheme owner will need to tailor this mechanism to best match the needs of their customers. Where appropriate, the label scheme owner should leverage existing software identification standards including, but not limited to:

1. Software ID Tags [[NISTIR 8060](#)]
2. Concise Software Identification Tags [[CoSWID](#)]
3. Common Platform Enumeration [[NISTIR 7695](#)]
4. Software Heritage persistent Identifiers [[SWHIDS](#)]
5. Package URL [[PURL](#)]

The scheme owner should also seek a mechanism that leverages both machine-readable and human-readable identifiers where appropriate.

Desired Outcome Consumers can clearly determine whether a given piece of software is described by a label and vice versa.

Assertions The claimant asserts to the completeness and correctness of the provided label-software linking information and this information conforms to the requirements established by the scheme owner.

2.2.1.4 Claim Date

Claim Claim Date

Description The date the label was issued. The granularity of this date should be defined by the scheme owner and should contain at minimum month and a year.

Desired Outcome Consumers can determine when a label's claims were made.

Assertions The claimant asserts the date provided corresponds to the claims conveyed by the label and that this date is accurate.

2.2.1.5 Security Update Status

Claim Security Update Status

Description A statement that details whether the software is being provided security related updates.

Desired Outcome When selecting software, the consumer should be able to determine whether a piece of software was being provided security related updates as of the claim date specified in the label. The consumer should understand that this claim is descriptive, and not necessarily a proactive claim of any commitment of any organization to continue to provide updates past the claim date.

Assertions The claimant asserts to the security update status of the software. This should take the form of one of two statements:

- **Supported** – the software was receiving security related updated as of the claim date.
- **Unsupported** – the software is no longer receiving security related updates.

The claimant asserts to make a good faith effort to update this claim when it is known the software will no longer receive security related updates.

2.2.1.6 Minimal Duration of Security Update Support

Claim	Minimal Duration of Security Update Support
Description	A clear statement of the duration during which the software will receive security related updates. This statement could be ‘unspecified’ if the claimant cannot or does not want to make statements concerning what a minimal duration of security update would be. The scheme owner will need to specify the granularity of this duration (e.g., whether statements are made to a specific day, month, or year). Furthermore, the scheme owner will need to make clear any liability concerns related to making this statement. Finally, the scheme owner should ensure that while updates to this claim may be made to extend the minimum duration, updates that shorten it are disallowed.

Desired Outcome Consumers should be able to quickly determine whether any proactive commitment has been made to provide security related software updates to the software, and if so, the minimum duration.

Assertions The claimant asserts one of the following duration claims:

- **Unspecified** – the claimant has chosen not to specify a minimum duration of support for security related software updates
- **Duration** – the claimant has described a minimum duration of commitment to provide security related software updates that conforms to the parameters as established by the scheme owner.

The claimant asserts to make a good faith effort to update this claim when it is known the software will no longer receive security related updates.

2.2.1.7 Security Update Method

Claim	Security Update Method
Description	A description of how security updates are provided to consumers for application to the software.
There are many mechanisms used to deliver security related updates. For example, mobile apps update through their respective app management ecosystems. Some software internally initiate and manage fetching updates. Still others require consumers to manually obtain new versions and install them manually. The consumer should be able to quickly distinguish between these mechanisms as they imply varying levels of personal responsibility concerning software maintenance.	
	The scheme owner should define the parameters for this description.
Desired Outcome	The consumer should clearly understand how security updates are administered and their personal role in the process.
Assertions	The claimant asserts the security update method described is accurate and complete and meets the criteria of the scheme owner.

2.2.2 Secure Software Development Claims

2.2.2.1 Implements a Secure Software Development Process

Claim	Implements a Secure Development Process
Description	The software development life cycles (SDLC) utilized for consumer software will vary depending on many factors. This claim assures that software has been built with security in mind and the processes implemented by the software developer meet the criteria established by the scheme owner. The scheme owner should establish criteria for secure development that correlate with appropriate practices and tasks identified in the NIST Secure Software Development Framework (SSDF) [SSDF] ² .
Desired Outcome	The consumer should be confident the software has been developed in accordance with industry accepted secure software development practices.

² See [Section 3.1.4](#) for a brief overview of the SSDF.

Assertions	The claimant asserts the software was developed using a process that adheres to the requirements established by the scheme owner.
-------------------	---

2.2.2.2 Practices Secure Design and Vulnerability Remediation

Claim	Practices Secure Design and Vulnerability Remediation
Description	<p>There are many best practices used in software development to minimize the occurrence and effect of vulnerabilities. Many of these are captured in the NIST SSDF. However, the following are recommended minimum practices and tasks:</p> <ul style="list-style-type: none">• Track and maintain the software's security requirements, risks, and design decisions (SSDF PW.1.2) [SSDF].• Review and/or Analyze Human-Readable Code to Identify Vulnerabilities and Verify Compliance with Security Requirements (SSDF PW.7) [SSDF].• Test Executable Code to Identify Vulnerabilities and Verify Compliance with Security Requirements (SSDF PW.8) [SSDF].• Analyze each vulnerability to gather sufficient information about risk to plan its remediation or other risk response (SSDF RV.2.1) [SSDF].• Plan and implement risk responses for vulnerabilities (SSDF RV.2.2) [SSDF].• Verifies that acquired commercial, open-source, and all other third-party software components meet defined security requirements (SSDF PW 4.4) [SSDF].• Ensure that high risk vulnerabilities publicly identified in the National Vulnerability Database [NVD], or other repository identified by the scheme owner, are remediated.
Desired Outcome	<p>Vulnerability detection and remediation is closely tied to the software developer's evaluation of risk and will vary depending on many factors across all classes of software. The scheme owner should identify suitable criteria for levels of consumer assurance.</p>
Assertions	Consumers should be confident when selecting software that reasonable steps have been taken to find and remediate vulnerabilities; however, they should understand that no process can ensure that software is vulnerability free.
Assertions	The claimant asserts in good faith that the software meets the minimum

criteria for vulnerability detection and remediation as established by the scheme owner and that any high-risk vulnerabilities have been remediated.

2.2.2.3 Practices Responsible Vulnerability Disclosure

Claim	Practices Responsible Vulnerability Disclosure
Description	Consumers should be informed of vulnerabilities that represent substantial risk to them. Task RV.1.3 in the NIST SSDF [SSDF] specifies that organizations: <i>Have a policy that addresses vulnerability disclosure and remediation, and implement the roles, responsibilities, and processes needed to support that policy.</i>
	The scheme owner will need to establish parameters surrounding the mechanisms used to disseminate this information to consumers, whether it be 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].
	Regardless of how this information is handled, its exact mechanism should be detailed for consumers who wish to access that information.
Desired Outcome	Consumers should be confident that vulnerabilities are reasonably reported to affected parties. Furthermore, the consumer should be easily able to discover how they can obtain information concerning these vulnerabilities.
Assertions	Vulnerabilities that put consumers at risk are disclosed through a clearly defined mechanism that meets the criteria of the scheme owner and this mechanism is clearly communicated to consumers.

2.2.2.4 Provides for Software Integrity and Provenance

Claim	Provides for Software Integrity and Provenance
Description	Practice PS.2 in the NIST SSDF [SSDF] identifies the need for consumers to have access to integrity verification mechanisms related to software. Examples of such mechanisms include, but are not limited to: <ul style="list-style-type: none">• <i>Post cryptographic hashes for release files on a well-secured website.</i>• <i>Use an established certificate authority for code signing so that consumers' operating systems or other tools and services can confirm the validity of signatures before use.</i>

- *Periodically review the code signing processes, including certificate renewal, rotation, revocation, and protection.*

The scheme owner should determine acceptable and appropriate mechanisms suitable for their customers.

Desired Outcome	Consumers should be confident that all software and subsequent updates are provided in a way that proves their authenticity and protects against tampering or counterfeiting by malicious actors.
------------------------	---

Assertions	The claimant asserts that a soft integrity and provenance mechanism exists and the details of how to obtain and use this information is available to consumers. Furthermore, this mechanism conforms to the mechanism(s) deemed appropriate by the scheme owner.
-------------------	--

2.2.2.5 **Uses Multifactor Authentication (if applicable)**

Claim	Uses Multifactor Authentication (if applicable)
Description	If the software requires or enables a human user to provide access to functionality or data, it should support multifactor authentication.
Desired Outcome	By examining the label, the consumer can quickly determine if the software provides multifactor authentication as a capability.
Assertions	The claimant makes one of the following assertions: <ul style="list-style-type: none">• Supports – The software supports multifactor authentication or participates in an identity federation ecosystem that supports multifactor authentication.• Not applicable – The software does not require user authentication

2.2.2.6 **Free from Hard-Coded Secrets**

Claim	Free from Hard-Coded Secrets
Description	The software does not store secrets utilized for encryption, passwords, or other authentication methods within the software.
Desired Outcome	Consumers should be confident that the software design does not enable attackers to easily gain unauthorized access to systems or data within the scope of the label.
Assertions	The claimant asserts the software does not contain hard-coded secrets.

2.2.2.7 **Uses Strong Cryptography**

Claim	Uses Strong Cryptography
--------------	--------------------------

Description	All cryptographic algorithms utilized by the software for security purposes follow NIST cryptographic standards and guidelines [CSG] at a minimum. Other approved cryptographic algorithms should be defined by the scheme owner.
Desired Outcome	Consumers should be confident that software is using modern and secure mechanisms to encrypt data, both at rest within the application as well as transmitted to and from the software.
Assertions	The claimant makes one of the following assertions:

- **Supports** – The cryptography implemented by the software for security related functions adheres to the cryptographic guidelines defined by the scheme owner.
- **Supports Externally** – The software relies on a system outside the label scope to provide for or enforce cryptographic functionality. This external system meets the guidelines defined by the scheme owner and the software has been designed to interface with this system in a way that meets the requirements defined by the scheme owner.

2.2.2.8 User Data is Identified and Secured

Claim	User Data is Identified and Secured
Description	<p>Software frequently must store, process, or transmit information that users consider to be sensitive, private, or of high value. This includes, but is not limited to:</p> <ul style="list-style-type: none">• Information 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.• Medical Information• Location information• Financial Information

A manifest should be provided that enumerates user data and details how said data is protected.

The criteria surrounding what qualifies as data appropriate for inclusion in manifest should be established by the scheme owner. The schema owner may wish to include or adapt existing user data classification efforts.

Desired Outcome Consumers should clearly understand what user data the software stores, processes, or transmits and how that data is protected.

Assertions The claimant asserts that a user data manifest is complete, accurate and relevant.

3 Labeling Criteria

This section describes the criteria for a cybersecurity labeling approach. These criteria are described as a set of label characteristics. Each has the following attributes:

- Characteristic – A unique, human-readable identifier for the characteristic
- Description – A definition for how the characteristic relates to a labeling approach
- Desired Outcome – The outcome and/or reasoning for including the characteristic in the label
- Components – A set of attributes, qualifiers, or supporting information that must be present in the labeling approach to satisfy the characteristic

The specific ways in which information is provided or who is responsible for providing the information (e.g., claimant or scheme owner) may vary depending on the final implementation of the labeling program.

Refer to [Appendix A](#) for more details behind these criteria and labeling considerations, including labeling approaches, consumer education, and consumer testing.

3.1 Binary Label

Characteristic	Binary label
Description	The product has a single, consumer-tested label indicating that the software has met the technical and conformity assessment criteria in the software labeling standard and when the product received the label.
Desired Outcome	The consumer should know that the software has met the criteria required to receive the label. The consumer can easily view the label before and at the time and point of software selection as well as at a later time, as needed. The consumer should know when the label was awarded.
Components	<p>The binary label has the following components:</p> <ul style="list-style-type: none">• Is available for consumers to view before and at the time and place of software selection as well as at a later time, as needed.• Supports physical or digital formats as appropriate depending on the manner in which the software can be selected.• The date (year at a minimum) when the label was asserted should be included on the label.• The claimant is using a label that has undergone rigorous consumer testing to ensure its usability.

3.2 Layered Approach

Characteristic	Implements a layered label approach
Description	The label provides a means for consumers to access additional information about the labeling program and the software's declaration of conformity.
Desired Outcome	The consumer has easy access to additional online information about the labeling program as well as declaration of conformity information for the software.
Components	<p>The label, as presented to consumers, provides a means for consumers to quickly and easily access additional online information. As a joint effort between partnering stakeholders (e.g., label scheme owner, manufacturers, industry and non-profit groups, government), the following additional information must be provided:</p> <ul style="list-style-type: none">• Consumer-focused information about the labeling program (see Appendix A – Consumer Education)• Declaration of conformity for the software, including the date of when the label was asserted• User data and data protection information contained in claim 2.2.2.8

4 Conformity Assessment Criteria

Conformity assessment is the term that describes the formalized process for demonstrating that specified requirements are fulfilled [ISO17000] A conformity assessment scheme consists of a set of rules and procedures that:

- describes the objects of conformity assessment (e.g., a consumer software);
- identifies the specified requirements (e.g., recommended criteria as defined in [Section 2.2](#) of this document);
- identifies the activity for performing conformity assessment (e.g., testing, inspection, certification, self-declaration of conformity, etc.); and
- defines roles and the types of organizations performing each role (e.g., first-, second- or third parties).

Given the range of consumer software and associated risks, **no single conformity assessment approach is appropriate**. This document does not recommend a particular set of conformity assessment requirements related to the recommended criteria. Rather, **NIST suggests that a scheme owner is necessary to tailor the recommended criteria, define conformity assessment requirements, develop the label and associated information, and conduct related consumer outreach and education**. Having a scheme owner facilitates fulfilling the primary objective of providing consumers with understandable and actionable cybersecurity-related information about the software.

There are several conformity assessment activities that could be leveraged in a consumer software scheme to demonstrate conformity to the recommended criteria, either exclusively or in combination. These include:

- Supplier's declaration of conformity (self-attestation) where the declaration of conformity is performed by the organization that provides the software. This is a self-attestation against a defined set of criteria.
- Third-party testing or inspection where there is determination or examination of the consumer software based on defined criteria.
- Third-party certification of the consumer software.

References

- [ANDREWS] Andrews JC, Burton S, Kees, J (2011) Is simpler always better? Consumer evaluations of front-of-package nutrition symbols. *Journal of Public Policy & Marketing* 30(2):175–190.
- [BLYTHE] Blythe JM, Johnson SD (2018) Rapid evidence assessment on labelling schemes and implications for consumer IoT security. *UK Department for Digital, Culture, Media & Sport Policy Paper*
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/949614/Rapid_evidence_assessment_IoT_security_oct_2018_V2.pdf
- [CMU] Carnegie Mellon University (2021) *IoT Security and Privacy Label*. Available at <https://iotsecurityprivacy.org/>
- [CoSWID] Birkholz, H., Fitzgerald-McKay, J., Schmidt, C., & Waltermire, D. (2021). Concise Software Identification Tags (Issue draft-ietf-sacm-coswid-19). Internet Engineering Task Force.
<https://datatracker.ietf.org/doc/html/draft-ietf-sacm-coswid-19>
- [CSG] National Institute of Standards and Technology (2021) *Cryptographic Standards and Guidelines*. Available at <https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines>
- [EMAMI-NAEINI-1] Emami-Naeini P, Dixon H, Agarwal Y, Cranor LF (2019) Exploring how privacy and security factor into IoT device purchase behavior. *CHI Conference on Human Factors in Computing Systems* (ACM, Glasgow, UK) , pp 1-12.
- [EMAMI-NAEINI-2] Emami-Naeini P, Agarwal Y, Cranor LF, Hibshi H (2020) Ask the experts: What should be on an IoT privacy and security label? *IEEE Symposium on Security and Privacy* (IEEE, Oakland, CA) pp. 447-464.
- [EO14028] Executive Order 14028 (2021) Improving the Nation's Cybersecurity. (The White House, Washington, DC), DCPD-202100401, May 12, 2021.
<https://www.govinfo.gov/app/details/DCPD-202100401>
- [EPA] Environmental Protection Agency (2021) *Energy Star Label*. Available at <https://www.energystar.gov/>
- [EU] European Commission (2021) *About the energy label and ecodesign*. Available at https://ec.europa.eu/info/energy-climate-change-environment/standards-tools-and-labels/products-labelling-rules-and-requirements/energy-label-and-ecodesign/about_en
- [FDA] U.S. Food and Drug Administration (2020) *The New Nutrition Facts Label*. Available at <https://www.fda.gov/food/nutrition-education->

[resources-materials/new-nutrition-facts-label](#)

- [FELT] Felt AP, Ha E, Egelman S, Haney A, Chin E, Wagner, D (2012) Android Permissions: User Attention, Comprehension, and Behavior. *Symposium on Usable Privacy and Security* (ACM, New York, NY) pp 3:1–3:14.
- [FINLAND] Finnish Transport and Communications Agency (2021) *Finnish Cybersecurity Label*. Available at <https://tietoturvamerkki.fi/en/>
- [FTC] Federal Trade Commission (2017) *The FTC “Lighting Facts” Label: Questions and Answers for Manufacturers*. Available at <https://www.ftc.gov/tips-advice/business-center/guidance/ftc-lighting-facts-label-questions-answers-manufacturers>
- [GARG] Garg, V (2021) A Lemon by Any Other Label. *International Conference on Information Systems Security and Privacy* (SCITEPRESS, Vienna, Austria) pp 558-565.
- [GOPAVARAM] Gopavaram, S, Dev, J, Das, S, Camp, LJ (2021) IoT Marketplace: Willingness-To-Pay vs. Willingness-To-Accept. *Annual Workshop on the Economics of Information Security*.
- [HARRIS] Harris Interactive (2019). Consumer Internet of Things Security Labelling Survey Research Findings.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950429/Harris_Interactive_Consumer_IoT_Security_Labelling_Survey_Report_V2.pdf
- [HODGKINS] Hodgkins CE (2016) Communicating healthier food choice – Food composition data, front-of-pack nutrition labelling and health claims. (Doctoral dissertation, University of Surrey, United Kingdom)
- [ISO9241] International Organization for Standardization/International Electrotechnical Commission (2018) *ISO 9241-11:2018 Ergonomics of human-system interaction – Part 11: Usability: Definitions and concepts* (ISO Geneva, Switzerland). Available at <https://www.iso.org/standard/63500.html>
- [ISO17000] International Organization for Standardization/International Electrotechnical Commission (2020) *ISO/IEC 17000:2020 Conformity Assessment — Vocabulary and General Principles* (ISO Geneva, Switzerland). Available at <https://www.iso.org/standard/29316.html>
- [ISO22603] International Organization for Standardization/International Electrotechnical Commission (2021) *ISO/IEC 22603-1:2021 Information technology — Digital representation of product information — Part 1: General requirements* (ISO, Geneva, Switzerland). Available at <https://www.iso.org/standard/73561.html>

- [JOHNSON] Johnson, SD, Blythe, JM, Manning, M, Wong, GT (2020) The impact of IoT security Labelling on consumer product choice and willingness to pay. *PloS One*, 15(1).
- [KLEEF] Kleef E Van, Dagevos H (2015) The Growing Role of Front-of-Pack Nutrition Profile Labeling: A Consumer Perspective on Key Issues and Controversies. *Critical Reviews in Food Science and Nutrition* 55(3):291–303.
- [KOENIGSTORFER] Koenigstorfer J, Wąsowicz-Kiryło G, Styśko-Kunkowska M, Groeppel-Klein A (2014) Behavioural effects of directive cues on front-of-package nutrition information: The combination matters! *Public Health Nutrition* 17(9):2115–2121.
- [NCSA] National Cybersecurity Alliance (2021) Oh, Behave! The annual cybersecurity attitudes and behaviors report 2021.
<https://staysafeonline.org/wp-content/uploads/2021/09/Oh-behave-The-Annual-Cybersecurity-Attitudes-and-Behaviors-Report-2021.pdf>
- [NHTSA] National Highway Traffic Safety Administration (2021) *Ratings*. Available at <https://www.nhtsa.gov/ratings>
- [NISTIR 7695] Cheikes BA, Waltermire DA, Scarfone KA (2011) Common Platform Enumeration: Naming Specification Version 2.3. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7695. <https://doi.org/10.6028/NIST.IR.7695>
- [NISTIR 8060] Waltermire DA, Cheikes BA, Feldman L, Witte GA (2016) Guidelines for the Creation of Interoperable Software Identification (SWID) Tags. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8060. <https://doi.org/10.6028/NIST.IR.8060>
- [NVD] National Institute of Standards and Technology (2021) *National Vulnerability Database*. Available at <https://nvd.nist.gov/>
- [PURL] (2021) *purl(Package URL)-spec*. Available at <https://github.com/package-url/purl-spec>
- [ROTHMAN] Rothman RL, Housam R, Weiss H, Davis D, Gregory R, Gebretsadik T, Shintani A, Elasy TA (2006). Patient understanding of food labels: the role of literacy and numeracy. *American Journal of Preventive Medicine* 31(5):391–398.
- [SINGAPORE] Cyber Security Agency of Singapore (2020) *Singapore's Cybersecurity Labelling Scheme*. Available at <https://www.csa.gov.sg/Programmes/cybersecurity-labelling-for-consumers>

- [SSDF] Souppaya M, Scarfone K, Dodson D (2022) Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-218. <https://doi.org/10.6028/NIST.SP.800-218>
- [STANTON] Stanton B, Theofanos MF, Prettyman SS, Furman S (2016) Security fatigue. *IT Professional*, 18(5):26-32.
- [STIFEL] Stifel M, Gilbert D, Peterson M (2019) Security Shield: A label to support sustainable cybersecurity. *Public Knowledge*.
<https://www.publicknowledge.org/blog/security-shield-a-label-to-educate-consumers-and-promote-sustainable-cybersecurity/>
- [SWHIDS] Software Heritage (2021) *SoftWare Heritage persistent IDentifiers (SWHIDs)* Available at <https://docs.softwareheritage.org-devel/swh-model/persistent-identifiers.html>
- [UL] UL (2021) *IoT Security Rating*. Available at <https://ims.ul.com/IoT-security-rating>
- [USABILITY] U.S. General Services Administration (2021) *Usability.gov*. Available at <https://www.usability.gov/>
- [USDA] U.S. Department of Agriculture (2021) *USDA Organic*. Available at <https://www.usda.gov/topics/organic>
- [VDP] National Institute of Standards and Technology (2021) *Vulnerability Disclosure Guidance*. Available at <https://csrc.nist.gov/projects/vdg>

Appendix A—Additional Context for Labeling Criteria

A.1 Introduction

The *software cybersecurity labeling provisions* in the May 12, 2021, Executive Order on Improving the Nation’s Cybersecurity (14028) aim to aid consumers in their software selection decisions by enabling comparisons among products and educating them about software security considerations. This transparency may also encourage providers to consider cybersecurity aspects of their software and ways to achieve greater consumer trust and confidence in the software, and ultimately, to improve the management of related cybersecurity risks.

A label’s impact on consumer software selection decisions can be influenced by multiple factors, such as time pressure when making a selection decision and competing priorities (e.g., software functionality and cost). A labeling program can facilitate the selection of more secure software by considering related needs and opportunities to educate consumers based on robust consumer-focused testing.

This appendix provides: an overview of different approaches to labeling; the NIST recommended approach for a software label; considerations for how the label might be provided to a consumer; how to mitigate potential issues with the recommended approach; consumer education considerations, and consumer testing and usability considerations.

These labeling recommendations are intended to support non-expert, home users of software. More technically detailed communication for expert users is out of scope for this document.

A.2 Methodology

In formulating consumer labeling and education considerations, NIST synthesized information related to labels and labeling programs from government, research, industry, and non-profit sources, including but not limited to position papers and input obtained during the [NIST Workshop on Cybersecurity Labeling Program for Consumers](#) on September 14-15, 2021, public comments on the [DRAFT Baseline Criteria for Consumer Software Cybersecurity Labeling](#), and the [NIST Cybersecurity Labeling for Consumer IoT and Software: Executive Order Update and Discussion](#) on December 9, 2021.

NIST also sought out lessons learned from real-world, market-tested labeling programs, including those administered by the Federal Trade Commission (FTC) and the Environment Protection Agency (EPA) Energy Star program, which is generally regarded as one of the most successful and recognizable government-administered programs.

Prior research findings on labels in both security and non-security fields were also considered, with more weight attributed to those studies that gauge actual consumer behavior in the

marketplace over those measuring self-reported intent, which may be subject to social acceptability bias³.

NIST further acknowledged and considered how the cybersecurity context may differ from other common label contexts (e.g., food or energy), such as the unclear return on investment for cybersecurity and cybersecurity concepts typically being poorly understood and not easily relatable among the general public [[STANTON](#)][[NCSA](#)].

Information and questions provided by other private and non-profit groups also provided important insights into potential consumer-related pitfalls and considerations when implementing cybersecurity labels.

A.3 Labeling Approaches

This section provides: an overview of different approaches to labeling; the NIST recommended approach for software labels (including considerations for how the label might be provided to a consumer); and how to mitigate potential issues with the recommended approach.

This document does not discuss specific label design elements, such as the use of icons, text, colors, or typography. However, when a label is eventually designed, **the usability of the label design as well as the usability of consumer education material should be assessed via rigorous consumer testing**. Usability and testing considerations are discussed in the Consumer Testing section later in this appendix.

A.3.1 Label Types

Labels are generally categorized into three types: descriptive, graded, and binary. Some variations or combinations of these may be used, especially with a layered approach in which a second layer of label detail can be obtained online.

A **descriptive** (or informational) label provides facts about properties or features of a product without any grading or evaluation. Information may be displayed in a variety of ways, such as in tabular format or with icons or text. Examples of descriptive labels in practice include [Nutrition Facts](#) [[FDA](#)] and [Lighting Facts](#) [[FTC](#)].

A **binary** label (sometimes called a “seal of approval”) is a single label indicating a product has met a baseline standard. Examples include [Energy Star](#) [[EPA](#)], [USDA Organic](#) [[USDA](#)], and the [government of Finland’s cybersecurity label](#) [[FINLAND](#)].

A **tiered** (or graded) label indicates the degree to which a product has satisfied a specific standard, sometimes based on attaining increasing levels of performance against specified criteria. Tiers or grades are often represented by colors (e.g., red-yellow-green), numbers of icons (e.g., stars or security shields), or other appropriate metaphors (e.g., precious metals: gold-silver-bronze). Examples include [vehicle safety ratings](#) [[NHTSA](#)] [UL IoT security rating](#) [[UL](#)], the [government](#)

³ Social acceptability bias is a tendency of people to answer questions in a way they think will be viewed favorably by others.

of Singapore's cybersecurity labeling scheme [[SINGAPORE](#)], and the European Union's energy efficiency letter grades [[EU](#)].

A *layered* label approach, while not a type of label per se, involves one of the three types of labels initially presented to the consumer with additional information or more detailed labels offered in supplementary (usually online) material. For example, a first-order product label may contain a reference to a website or a Quick Response (QR) code that takes a consumer to more detailed information online. An example of a layered label is [CMU's proposed IoT Security and Privacy Label \[CMU\]](#).

A.3.2 Recommended Label Approach

In recommending an approach for software cybersecurity labeling, NIST relied on the following guiding principles:

1. The labeling approach should be appropriate to the proposed software cybersecurity label technical criteria.
2. The labeling approach should be usable by a diverse range of consumers without requiring them to have specialized cybersecurity knowledge.

Recognizing that all labeling approaches have their strengths and weaknesses, **NIST recommends that a binary label (a single label indicating a product has met a baseline standard) should be adopted for a software cybersecurity label.**

NIST recommends that the software label be based on a declaration of conformity with specific product criteria. This negates the value of a *descriptive label*, which relies on consumer interpretation of what is acceptable [[ROTHMAN](#)].

A *tiered label* is not suitable because the recommended product criteria consist of a single, minimum baseline. If tiers are introduced in the future to include further criteria – for example, additional product criteria defined by increasing perceived risk, additional testing tools in product assessment, or independent testing beyond self-certification – the label can then be adjusted.

Binary labels are generally considered more usable and are often preferred by consumers over other alternatives [[BLYTHE](#)][[JOHNSON](#)]. In an IoT cybersecurity label study, binary cybersecurity labels had a positive effect on purchase intention [[JOHNSON](#)]. Moreover, the simplicity of binary labels results in less cognitive burden as compared to descriptive and graded labels [[KOENIGSTORFER](#)] since the label does not rely on consumers having to determine which properties or tiers are most appropriate and important for their own context of use [[GARG](#)][[FELT](#)][[EMAMI-NAEINI-2](#)]. This simplicity is especially needed within the cybersecurity context given the diversity of software consumers, with many lacking expertise in cybersecurity risks, mitigations, and consequences. Overall, binary labels are more effective in those situations – such as the software selection context – in which consumers may lack the time, expertise, or desire to be presented with more information [[HODGKINS](#)].

NIST also recommends coupling the binary label with a layered approach in which one of the following is included on the label to lead consumers to additional details online:

- a URL (e.g., as included in Singapore’s cybersecurity label [[SINGAPORE](#)]), not a shortened URL, which is not easily attributed to the source domain
- a scannable code (e.g., a QR code).

Layered labels can help with consumer education about the labeling effort, provide a means to access the product’s declaration of conformity, and enable comparison to other labeling schemes (e.g., those used in other countries). Layers have the advantage of potentially satisfying the information needs and wants of a wide range of cybersecurity expert and non-expert consumers, some of whom research has revealed want to learn more about what is behind cybersecurity labels [[EMAMI-NAEINI-1](#)][[JOHNSON](#)]. Those who do not care to know more need not be exposed to the details, while those who desire more information can access another layer of information.

While access to a second layer should be quick and easy, it is unclear how willing consumers may be to scan a QR code or visit a website to obtain additional information, or whether consumers will have access to technology that will allow them to scan a QR code. Therefore, consumer testing in this regard will be essential. In addition, the potential security risks of QR codes should be carefully investigated prior to including them on a label.

A.3.3 Label Presentation

Label presentation – how and where a label is presented to consumers – is another important consideration. **Labels should be available to consumers before and at the time and place of software selection (in-store or online) as well as after selection.** Therefore, a software cybersecurity label should be flexible in supporting both physical and digital formats as appropriate.

Physical labels on software packaging may not be appropriate for all software (e.g., for those with small packaging). If appropriate, physical labels should follow applicable labeling standards and be located on a conspicuous, but not intrusive, place [[STIFEL](#)][[JOHNSON](#)]. The date or year of when the product received the label should also be included.

Digital labels (e-labels) (e.g., as described in the ISO/IEC electronic labelling standard [[ISO22603](#)]) should be available for all products for several reasons.

- These labels can serve as an additional layer of detail for physical labels when utilizing a layered approach.
- Digital labels also provide a means for consumers to view current label status after selection or after transfer of product ownership.
- E-labels allow for labeling to be dynamic, reflecting changes in the product lifecycle or cybersecurity status due to changing risks [[STIFEL](#)].
- Digital labels with a machine-readable component may be used at some point in the future by security vendors, tools, auditors, and service providers to automatically assess the vulnerability of software products and prompt consumers to remediate issues.

The presentation and framing of the labels in the marketplace should also be carefully considered. For example, in one research study, displaying products in order from highest to lowest privacy

rating encouraged consumers to select more highly-rated products, even when those products cost more [[GOPAVARAM](#)]. As retailers and software providers are often the first point of contact for consumers, they should be engaged as active partners in label delivery.

A.3.4 Addressing Potential Weaknesses

There are potential weaknesses of any labeling approach with respect to consumer perceptions. NIST recognizes that in a voluntary cybersecurity labeling scenario, binary labels may lead to dichotomous thinking in which a product with a label is considered “good” while products without a label are considered “bad” [[JOHNSON](#)][[KLEEF](#)][[ANDREWS](#)]. In reality, **the presence or absence of a voluntary label would not necessarily indicate better cybersecurity attributes or increased risk**. Dichotomous thinking may be compounded if the voluntary labeling is not widely adopted among software vendors.

There is also a concern about potential “halo” effects – the tendency for creating a positive impression of a product based on the fact it has a label [[ANDREWS](#)]. In the cybersecurity label context, a halo effect would be a false sense of security. However, recent studies related to IoT cybersecurity labels have shown that consumers generally understand that labeled products are not 100% secure, with the halo effect only manifested in a small minority of consumers [[JOHNSON](#)][[HARRIS](#)]. Since this research was conducted in the UK, a similar study is likely warranted to gauge interpretations of U.S. consumers.

To counter the potential of dichotomous thinking or halo effects, binary labels should be accompanied by a robust consumer education campaign (see Consumer Education below). This education campaign is also necessary to build brand recognition since binary labels (especially for new or lesser-known labels) may fail to garner consumer attention [[KOENIGSTORFER](#)], and the effectiveness of binary labels is highly correlated with familiarity [[GARG](#)].

A.4 Consumer Education

As a complement to the labeling approach, a robust consumer education program should be developed to establish and increase label recognition, provide transparency to consumers about important aspects of the labeling program, and ensure a common way for software stakeholders to talk about the labels. *Who* provides this information will be dependent on the final construct of the labeling program. **Because consumer education will be an involved undertaking, it should be a shared responsibility among multiple software security stakeholders** (e.g., scheme owners, retailers or software providers who are often the first point of contact for consumers, manufacturers, industry and non-profit security groups, academia, or the government).

Note that although this section describes education materials for consumers, **education for manufacturers, retailers, and software providers is also of great importance** and can borrow from the consumer education materials as much as possible to ensure consistency.

At a minimum, consumers should have online access – not necessarily included in the label itself – to the following information:

- Intent and scope – What the label means and does not mean, including addressing potential misinterpretations (e.g., stating that a secure development process reduces risk but does not eliminate it entirely and that labeled products are not necessarily more secure than unlabeled products); inclusion of a statement that a label does not imply product endorsement by the label program
- Product criteria – What cybersecurity properties are included in the baseline and why and how these were selected; include information on how the criteria address security risks both to the consumer and to others (e.g., if co-opted into a botnet) for common intended uses of the products
- A glossary of applicable technical terms, written in plain language
- General information about conformity assessment – How cybersecurity properties are evaluated
- Declaration of conformity – The product’s specific declaration of conformity to the baseline criteria, including the date the label was last awarded
- User Data – The information described in [section 2.2.2.8](#) that describes what sensitive data is handled by the software and how that data is protected.
- Scope – The kinds of products eligible for the label and an easy way for consumers to identify labeled products
- Changing applicability – The current state of product labeling as new cybersecurity threats and vulnerabilities emerge
- Expectations for consumers – The responsibility consumers share in securing software and how their actions (or inactions) can impact the software’s cybersecurity
- Contact information for the labeling program and information on how consumers can issue a complaint against a vendor regarding a product label

Particular care should be taken with the messaging and framing of consumer education material. Similar to the layered label approach described above, **a layered approach for consumer education materials is recommended** as it allows for basic information in a first level of consumer education material with links to more detail if desired.

Most information (with the exception of detailed technical information, e.g., declaration of conformity) should be accessible to a wide range of consumers and be presented using language that is understandable to non-experts, typically written at no more than an 8th grade reading level, for example, in accordance with the specifications in the Plain Writing Act of 2010⁴. Translations of education materials into common languages spoken in the U.S. should be provided to support the substantial number of consumers who are not proficient in English. In addition to static web page text, the use of multiple formats, such as video and audio, may also foster public

⁴ <https://www.plainlanguage.gov/law/>

understanding and be more accessible (e.g., compliant with Section 508 of the Rehabilitation Act) for consumers of differing abilities.

Given that many consumers may not fully appreciate cybersecurity threats and vulnerabilities – and their software product’s related risks and susceptibility – the application of risk communication principles can be especially helpful for establishing the importance and relevance of the label. Tying cybersecurity to non-cybersecurity benefits (e.g., availability, reliability) may be valuable in establishing relevance.

To facilitate brand recognition among a demographically diverse population, ideally a public education campaign should be launched via a variety of communication channels, including web sites, social media, and news outlets. A study related to IoT cybersecurity labels commissioned by the UK Government identified potential outlets appropriate to various demographic groups [[HARRIS](#)]. Similar market research for a U.S. population would be informative and should be prioritized.

A.5 Consumer Usability and Testing

Beyond proposing a suitable label scheme and considerations for consumer education, *a specific label design* is out of scope for this document since design selection ideally would be based on extensive consumer testing. Instead, this section describes considerations for usability and consumer testing for a consumer software cybersecurity label.

A.5.5 Usability Considerations

Usability is “the extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use” [[ISO9241](#)]. Applying this definition within the context of consumer cybersecurity labels, the “system, product, or service” is the label itself. “Users” are synonymous with software consumers. For the cybersecurity labeling effort, the primary goal is for consumers to be informed about software cybersecurity capabilities when making purchase decisions. “Context of use” refers to the conditions under which a label will be used, the characteristics of the consumer, and how the consumer will use the label (label-related tasks).

“Effectiveness, efficiency, and satisfaction” are the foundational components of usability. In addition, usability.gov [[USABILITY](#)] references two other factors contributing to efficiency which are relevant: ease of learning and memorability. Table 2 lists usability components along with a brief description of each and potential considerations for consumer cybersecurity labels. The label design should also account for *accessibility* factors that may significantly impact and overlap with the usability components listed, for example, when used by consumers with disabilities or the aging.

Table 1: Usability components as applied to consumer cybersecurity labels

Usability Component	Description	Consumer Cybersecurity Label Considerations
Effectiveness	Accuracy and completeness with which consumers can achieve their goals	<p>Label components are appropriate for supporting consumer goals.</p> <p>Consumers should be able to accurately interpret the label's meaning and successfully compare two or more products to determine which has met a baseline level of cybersecurity using relevant standards and criteria.</p> <p>Consumers should not be presented with information that is beyond the average consumer's skill level or which requires significant study to appreciate.</p> <p>Elements of the label – e.g., symbols, icons, text, or colors – should be commonly understood by most consumers in the U.S. and potentially beyond.</p> <p>The label and education materials should be accessible to those with differing abilities (e.g., by meeting the requirements of Section 508 of the Rehabilitation Act).</p>
Efficiency	Resources used in relation to the results achieved	<p>Consumers should be able to quickly gain a broad sense of the product's cybersecurity level without being required to seek out additional information.</p> <p>There should be an easy, quick way or ways for the consumer to get more details about the label, the product's security performance, and the labeling program for consumers who may want that option.</p>
	Ease of learning: how fast a consumer who has never seen the label before can accomplish basic tasks	<p>The label should have a minimalistic design and be understandable by those without expertise in cybersecurity or information technology. Any icons should be coupled with a mechanism for consumers to look up the definitions of each icon online in multiple languages.</p> <p>Documentation should be described in plain language suitable for most consumers. Since</p>

Usability Component	Description	Consumer Cybersecurity Label Considerations
		consumers are diverse, those consumers who wish to seek out additional details about the criteria behind the label can be referred to a technical criteria reference.
	Memorability: after being exposed to/using the label, whether a consumer can remember enough to use it effectively in the future	Even in the potential case of multiple label scheme owners, the label should be standardized to facilitate eventual widespread recognition and allow consumers to make uniform comparisons across similar products.
Satisfaction	Extent to which the consumer's physical, cognitive, and emotional responses that result from the use of the label meet the consumer's needs and expectations	Consumers should perceive the labels as value-added, understandable, and useful in their product selection decisions. Consumers should also perceive the label as aesthetically/visually appropriate.

A.5.6 Consumer Testing

To determine a label’s usability, selected label designs and consumer education materials should undergo rigorous consumer testing prior to launching a labeling program. While a label scheme owner will likely oversee consumer testing efforts, these may be conducted in partnership with other stakeholders, e.g., academia, industry, and non-profits.

Usability testing evaluates the components outlined in Table 2. Those testing methods may vary. For example, in the early design phase, a “within subjects” usability test, in which people are shown more than one possible design, could determine preference among multiple designs. After the choices of possible designs are narrowed down, candidate designs may be compared and evaluated in a “between-subjects” usability test in which each participant sees only one label design, performs a series of tasks (like providing an interpretation of the label or comparing products), and answers subjective satisfaction questions after the tasks. Findings regarding potential consumer misconceptions or preferences can be incorporated into a revised design or targeted for consumer education materials. Consumer education materials should also be subject to consumer testing to ensure their usability.

There is also value in studying – before a program is launched – the potential impact of the label on consumers’ actual software selection decisions to gauge whether a labeling program achieves the EO’s stated goals. For example, because certain psychological biases (e.g., halo effect) may affect consumers’ decision making, a deeper understanding of consumers’ perceptions of the labels, the potential impact of biases on selection decisions, and possible strategies for encouraging consumers to select more secure products will be critical to the success of a labeling program. In

addition, pre-launch consumer testing should begin to gauge the level of trust consumers may have in the labels, including perceived credibility of the technical criteria, program administrator, and conformity assessment method.

Consumer testing prior to program implementation is valuable, but initial perceptions and expressions of intent to select software may differ from actual consumer behavior. Therefore, **periodic testing after program implementation is essential** and can include market studies to assess the continued appropriateness and usability of the label approach, impact on consumer software selection decisions, and the growth of brand recognition over time.

Including a demographically diverse, U.S. census-representative sample of consumers of varying disabilities and abilities in the pre-launch and periodic, post-launch testing is critical for determining that the label is broadly understandable and ensuring testing results are not biased. The sample size should be large enough for sufficient statistical power when analyzing test results.

Appendix B—Abbreviated SSDF Example

Table 2: Abbreviated example from the SSDF

Practice	Tasks	Notional Implementation Examples	References
Respond to Vulnerabilities (RV)			
Identify and Confirm Vulnerabilities on an Ongoing Basis (RV.1): Help ensure that vulnerabilities are identified more quickly so that they can be remediated more quickly in accordance with risk, reducing the window of opportunity for attackers	RV.1.1: Gather information from software acquirers, users, and public sources on potential vulnerabilities in the software and third-party components that the software uses, and investigate all credible reports.	<p>Example 1: Monitor vulnerability databases, security mailing lists, and other sources of vulnerability reports through manual or automated means.</p> <p>Example 2: Use threat intelligence sources to better understand how vulnerabilities in general are being exploited.</p> <p>Example 3: Automatically review provenance and software composition data for all software components to identify any new vulnerabilities they have.</p>	BSAFSS: VM.1-3, VM.3 BSIMM: AM1.5, CMVM1.2, CMVM2.1, CMVM3.4, CMVM3.7 CNCFSSCP: Securing Materials—Verification IEC62443: DM-1, DM-2, DM-3 ISO29147: 6.2.1, 6.2.2, 6.2.4, 6.3, 6.5 ISO30111: 7.1.3 OWASPSAMM: IM1-A, IM2-B, EH1-B OWASPSCVS: 4 PCISSL: 3.4, 4.1, 9.1 SCAGILE: Operational Security Task 5 SCFPSSD: Vulnerability Response and Disclosure SCTPC: MONITOR1 SP80053: SA-10, SR-3, SR-4 SP800161: SA-10, SR-3, SR-4 SP800181: K0009, K0038, K0040, K0070, K0161, K0362; S0078