DRAFT Baseline Criteria for Consumer Software Cybersecurity Labeling

November 1st, 2021

Comments on this draft document are due by December 16, 2021 and can be emailed to labeling-eo@nist.gov**.** Please submit comments along with the submitter's name and organization (if any) and use the subject "**Draft Consumer Software Labeling Criteria.**" Receipt of submissions will be acknowledged by email, and all comments will be published at https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/consumer-software-criteria.

Note for Reviewers:

This draft document advances assignments to the National Institute of Standards and Technology (NIST) in Sec. 4 (s) of Executive Order (EO) 14028, "Improving the Nation's Cybersecurity" related to cybersecurity labeling for consumer software. It complements a similar document addressing cybersecurity-related consumer labeling for Internet of Things (IoT) products. The criteria in this document are based on extensive input offered to NIST in a September 2021 workshop and position papers submitted to NIST, along with the agency's research and discussions with organizations and experts from the public and private sector. In accordance with the EO, NIST plans to produce a final version of these criteria by February 6, 2022.

NIST seeks comments on all aspects of the criteria contained in this draft document, including:

- 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.
- 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.
- Whether the labeling-specific criteria are appropriate and likely to be effective for consumers.
- 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.
- Whether additional considerations for the labeling approach, consumer education, or testing are needed – including:
    - Possible appropriate definitive text for describing the labeling program in consumer education materials
    - Best approaches for addressing the needs of non-English speaking consumers
- 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.
- Whether the conformity assessment provisions are appropriate.
- Whether a template Declaration of Conformity would be useful for software providers.
- Whether more details on evidence required to support assertions would be useful for software providers.
- Whether the technical baseline criteria are appropriate, including but not limited to:
    - The feasibility, clarity, completeness, and appropriateness of attestations

- Normative references to be considered for inclusion
- Potentially requiring that the Software Identifiers attestation take the form of a Software ID Tags

1 Introduction

1.1 Background

Sec. 4 (s) of 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, Sec. 4 (u) of the EO directs NIST to **"…identify secure software development practices or criteria for a consumer software labeling program…**." Furthermore, the identified criteria "…shall reflect a baseline level of security practices, and if practicable, shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone."

Sec. 4 (u) also states that "...NIST shall 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 advances 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 well be unclear. While enabling many benefits to consumers, that software – that is, **software normally used for personal, family, or household purposes –** also is subject to 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 which will improve consumers' awareness, information, and ability to make purchasing decisions while taking cybersecurity considerations into account. The criteria in this document have the following primary specific goals:

- Establish a baseline set of technical criteria to inform the responsibilities of consumer software providers[1] and a software label. These should 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 which attest to labeling software

This document references existing resources, standards, and programs that may satisfy, complement, or enable the established criteria without repeating them here. These criteria are intended to complement and not to conflict with the IoT Product Criteria which meet the goals of Sec. 4 (t).

It is important to stress that these criteria set 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 program for consumer software. Rather, these criteria set out desired outcomes, allowing and enabling the marketplace of providers and consumers to make informed choices.

NIST plans to identify opportunities for advancing consumer education about cybersecurity of consumer software via labels and to consider how these efforts incentivize consumer software providers to improve the cybersecurity aspects of their products and in consumer purchasing decisions.

1.3 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 – details a proposed approach for conformity assessment

[1] The term software provider is explained in Section 2.2 below

- Appendix A – provides additional details on labeling criteria and considerations, including labeling approaches, consumer education, usability, and consumer testing

2 Baseline Technical Criteria Associated with Labels

2.1 Methodology

This section describes the technical criteria as a series of *attestations*, or claims made about the software associated with the label. When referenced by the label, the consumer is informed about these *outcome-based* assertions and associated information. This is consistent with the conformity assessment methodology Supplier's Declaration of Conformity, or SDOC, which also is referred to as a Self-Declaration of Conformity. Additional information about conformity assessment related to consumer software labeling appears in Section 4.

The attestations are organized into four categories:

1. **Descriptive Attestations** – 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 attestations were made, and how a consumer can obtain other supporting information required by the label.
2. **Secure Software Development Attestations** – This category describes how the software provider adheres to accepted secure software development practices throughout the software development lifecycle. By fulfilling criteria in this category, the provider of software communicates to the consumer that recommended secure software development practices were employed.
3. **Critical Cybersecurity Attributes and Capability Attestations** – This category describes certain features expressed by the software that should result from implementing a secure software development process.
4. **Data Inventory and Protection Attestations** – This category makes declarations concerning data that is stored, processed, or transmitted by the software. This category has two primary objectives:
    a. Enumerating data types that consumers may identify as having high cybersecurity-related risk and allowing the software developer to describe mechanisms they have used to safeguard that data.
    b. Enumerating types of data that the software developer has spent time and effort safeguarding and wishes to communicate to the consumer.

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

2.2 Terminology Conventions

The Descriptive Attestation group defines two terms, **Software Provider** and **Label Scope:**

A **Software Provider** has been defined in broad terms to encompass organizations of varying sizes and functions. This allows for individual developers, developer organizations, publishers, and others to satisfy this attestation specification if they have the authority to make such attestations.

The **Label Scope** attestation refers to what a label is describing. This allows a software provider 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."

2.3 Baseline Criteria

This section describes all attestations included in the baseline criteria. For each attestation, this document defines the following attributes:

- Attestation – A unique, human-readable identifier for the attestation
- Description – A statement about what information the attestation should capture
- Desired Outcome – The outcome and/or reasoning for including the attribute in the label
- Assertions – The criteria for satisfying the attestation requirement.

In order to label consumer software or otherwise indicate that it conforms to the criteria in this document, the software provider must address all the baseline criteria. Several of the criteria address characteristics that may not be included in a specific consumer software product. Those criteria allow the software provider to assert that the attestation is not applicable. A summary of each category and the names of each of the attestations appears below:

1. Descriptive Attestations
    - *Software Provider*
    - *Label Scope*
    - *Software Identifiers*
    - *Attestation Date*
    - *Software End of Support Date*
    - *Vulnerability Reporting*
2. Software Development Attestations
    - *Implements A Secure Development Process*
3. Critical Cybersecurity Attributes and Capability Attestations
    - *Free from Known Vulnerabilities*
    - *Software Integrity and Provenance*
    - *Multifactor Authentication (if applicable)*
    - *Free from Hard Coded Secrets*
    - *Strong Cryptography (if applicable)*
4. Data Inventory and Protection Attestations
    - *Personally Identifiable Information (PII) Data Manifest (if applicable)*
    - *Location Data Manifest (if applicable)*
    - *Application Specific Data Manifest*

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

2.3.1 Descriptive Attestations

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.

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.

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.

2.3.1.4 Attestation Date

Attestation	Attestation Date
Description	The date the label was issued.
Desired Outcome	Consumers can determine when the label's attestations were made.
Assertions	The date on which the software provider makes the claims contained within the label is accurate and made readily available to the consumer.

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.

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].

2.3.2 Software Development Attestations

2.3.2.1 Implements a Secure Development Process

Attestation	Implements a Secure Development Process
Description	The software provider implements a development process that is consistent with the NIST Secure Software Development Framework (SSDF) [SSDF].
Desired Outcome	The consumer should be confident the software developer has used accepted secure software development practices throughout the software development lifecycle.

Assertions	The software provider uses a secure development process that includes all applicable practices contained in the NIST SSDF[SSDF].

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.

2.3.3.2 Software Integrity and Provenance

Attestation	Software Integrity and Provenance
Description	The software and all provided updates are cryptographically signed by the software provider.
Desire 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 software provider asserts that all software is cryptographically signed and provides a mechanism for consumers to verify the software they are using has not been tempered with.

2.3.3.3 Multifactor Authentication

Attestation	Multifactor Authentication
Description	If the software requires or enables a human user to provide access to functionality or data, it should also 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 software provider makes one of the following assertions: • **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

2.3.3.4 Free from Hard-Coded Secrets

Attestation	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 software provider asserts no software contains hard-coded secrets.

2.3.3.5 Strong Cryptography

Attestation	Strong Cryptography
Description	All cryptographic algorithms utilized by the software follow NIST cryptographic standards and guidelines [CSG].
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 software provider makes one of the following assertions: • **Supports** – The software natively utilizes NIST approved cryptographic standards and follows all related guidelines. • **Not Applicable** – The software relies on a system outside the purview of the software to provide for or enforce data encryption. For example, the software may rely on the mobile operating system to provide for and enforce data encryption for data at rest.

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.
    - Social security numbers, passport numbers or any similar official ID number
    - Banking, financial, or medical account numbers
    - Medical information
- **Not Applicable –** The software does not store, process, or transmit any PII data.

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.

2.3.4.3 Application-Specific Data Manifest

Attestation	Application-Specific Data Manifest
Description	Application-Specific Data is any data not captured in the previous attestations. A software provider may wish to communicate any safeguards they have implemented to the consumer.
Desired Outcome	Consumers should be able to understand and differentiate the safeguards utilized by software that involve similar data. Software providers can differentiate their software from competitors.
Assertions	The software provider contains a manifest of any Application Specific Data and any safeguards implemented by the software provider to protect said data. Note, this field **MAY** be empty.

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., software providers or labeling program administrator) 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 at the time and point of purchase as well as at a later time, as needed. The consumer should know when the label was awarded.
Components	The binary label has the following components: • Is available for consumers to view at the time and place of purchase as well as at a later time, as needed. • Supports physical or digital formats as appropriate depending on the manner by which the software can be purchased. • The date (year at a minimum) when the label was asserted should be included on the label. • The software provider 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	The label, as presented to consumers, provides a means for consumers to quickly and easily access additional online information. The following additional information must be provided: • 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 • Data Inventory and Protection Attestation descriptions

4 Conformity Assessment Criteria

This section defines the conformity assessment criteria for consumer software cybersecurity labeling. The conformity assessment criteria defined below are based on the concept of Supplier's Declaration of conformity. A Supplier's Declaration of Conformity (SDOC, also, sometimes called Self Declaration of Conformity) is one way to show that a product, process, or service conforms to a standard or technical regulation the supplier uses a the SDOC to provide written assurance of conformity to the specified requirements. The declaration normally is a separate document. For purposes of the criteria in this document, the supplier is the software developer. The software provider has the option of using an accredited laboratory or inspection body, which would be indicated on the declaration; this is not a requirement. The choice of where to test is left to the software provider. Organizations interested in labeling consumer software may use the criteria to map to existing or to new programs. Programs that meet all relevant criteria may make an associated claim when labeling consumer software.

In developing the conformity assessment process for consumer software cybersecurity labeling, NIST considered comments and feedback in requested position papers, during the September workshop, as well as via other stakeholder engagements. For this section, the conformity assessment terms utilized are based on:

- ISO/IEC 17050 Part 1: Conformity Assessment – Suppliers Declaration of Conformity, Part 1: General Criteria[2].
- ISO/IEC 17050 Part 2: Conformity Assessment – Suppliers Declaration of Conformity, Part 2: Supporting Documentation.

[2] ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) are international standards organizations and work together on international standards related to conformity assessment topics.

The declaration of conformity shall include the following:

1. Purpose of the declaration of conformity

    - The software provider shall attest that the consumer software meets the requirements both in function and operating environment to the specified software technical requirements.
    - If the software provider has a program that utilizes other conformity assessment activities, such as testing or inspection, those results can be included in the attestation for purposes of ensuring consumer software requirements meet specified requirements.

2. General requirements

    - The software provider shall maintain procedures for issuing, maintaining, extending, reducing, suspending, or withdrawing the declaration as well as the attestation of the consumer software.
    - The software provider shall have procedures in place to ensure the continued conformity of the software development practice as acknowledged to the specified technical criteria within the declaration of conformity.
    - The software provider should maintain separation of responsibilities and role between the person conducting the review of the attestation and the signatory of the consumer software attestation.

3. Contents of the declaration of conformity

    - The software provider shall ensure that the declaration of conformity for consumer software contains all required information to enable consumers or any organization receiving the declaration to clearly identify specified requirements to which conformity is declared.
    - The declaration shall include, at a minimum, the following:
        - Unique identification of the declaration;
        - Unique identification of the software identifier attestation as defined in Section 2.3 Baseline Criteria, Clause 2.3.1.3 Software Identifiers;
        - Name and contact information of the software provider as defined in Section 2.3 Baseline Criteria, Clause 2.3.1.1 Software Provider;
        - Clear identification of the software product name as defined in Section 2.3 Baseline Criteria, Clause 2.3.1.2 Label Scope;
        - Clear identification of the secure software development process as defined in Section 2.3 Baseline Criteria, Clause 2.3.2.1 Implements a Secure Development Process;
        - Statement of conformity that software provider meets specified technical criteria;
        - List of specified technical criteria that software provider attests conformity in Section 2.3 Baseline Criteria;
        - Date and location that declaration created as defined in Section 2.3 Baseline Criteria, Clause 2.3.1.4 Attestation Date;
        - Signature of authorized individual acting on behalf of the software provider including name and title as defined in Section 2.3 Baseline Criteria, Clause 2.3.1.1 Software Provider; and
        - Any limitations on the validity of the declaration of conformity.

4. Supporting documentation – If using a third-party conformity assessment program to supplement the declaration of conformity, the following criteria also apply.

- To support the declaration of conformity results, additional supporting information may be provided including:
    - Name and contact information of the conformity assessment body;
    - Date and reference to report from conformity assessment body;
    - Reference to accreditation documentation of the conformity assessment body where the scope of accreditation is relevant to consumer software declaration and secure software development specified requirements, if applicable;
    - Information about certificates or marks obtained from the conformity assessment body.
- Supporting documentation shall be developed, controlled, and maintained in a manner to allow traceability from the consumer software requirements;
- The software provider shall have procedures in place to ensure the retention period of supporting documentation in accordance with applicable laws and regulations as well as ensure specific needs of consumers and other interested parties are considered.
- The supporting documentation shall include the following information to demonstrate conformity of the consumer software with the declared requirements within 3. – Contents of declaration of conformity:
    - Description of the consumer software;
    - Description of the secure development process and applicable technical criteria;
    - Conformity assessment results including:
        - Description of the attributes used,
        - Results, and
        - Evaluation of the results including any deviations.
- Identification, qualifications, and technical competence of the conformity assessment body involved as well as their accreditation status including scope and name of the accreditation organization.

Appendix A: Additional Context for Labeling Criteria

Introduction

From a consumer perspective, 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 purchase decisions by enabling comparisons among products and educating consumers on software security considerations. This transparency is intended to encourage providers to consider cybersecurity aspects of their software and greater consumer trust and confidence in the software and ultimately, improved management of related cybersecurity risks.

A label's impact on consumer purchase decisions can be influenced by multiple factors, such as time pressure at the point of purchase and competing priorities (e.g., software functionality and cost). A labeling program can facilitate the purchase of more secure software by considering related needs and opportunities to educate consumers based on robust consumer-focused testing. This appendix addresses considerations for these consumer-focused components of approaches to labeling.

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. When considering sources, NIST assigned greater weight to experiences and 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 bias[3]. NIST further 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.

Labeling Approaches

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

This section provides an overview of different approaches to labeling, the NIST proposed approach for software labels (including considerations for how the label might be provided to a consumer), and how to mitigate potential issues with the proposed 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, care should be taken to assess the usability of these elements; usability considerations are discussed in the Consumer Testing section later in this appendix.

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 ***graded*** (tiered) label indicates the degree to which a product has satisfied a specific standard, sometimes based on attaining increasing levels of performance against specified criteria. Grades or tiers 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 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].

Proposed Label Approach

In proposing 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.

All labeling approaches have their strengths and weaknesses. Taking those into account within the anticipated context of the software security label, **NIST proposes that a *binary label* is likely most**

appropriate. A graded label is not suitable because the proposed technical criteria consist of a single, minimum baseline. However, if additional levels of attestation or technical criteria are added in the future, the label can be adjusted. Furthermore, since NIST is proposing that the software label technical criteria will be based on a declaration of conformity, this negates the value of a descriptive label, which relies on consumer interpretation of what is acceptable [ROTHMAN].

With respect to the second principle of usability for diverse consumers, 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*, although somewhat less so than descriptive or graded labels [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 cybersecurity expertise. Overall, binary labels are more effective in those situations – such as the software purchase context – in which consumers may lack the time, expertise, or desire to be presented with more information [HODGKINS].

NIST also is proposing coupling the binary label with a *layered approach* in which a short URL (as included in Singapore's cybersecurity label [SINGAPORE]) or scannable code (e.g., a QR code) on the binary label leads consumers to additional details online. Layered labels can help with consumer education about the labeling effort and provide a means to access the software's declaration of conformity. 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-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, so consumer testing in this regard will be essential.

Label Presentation

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

Physical labels on software packaging 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. First, they may be especially appropriate given software products are often downloaded from online marketplaces. These labels can also serve as an additional layer of detail for physical labels (if used) when utilizing a layered approach. Digital labels also provide a means for consumers to view current label status after purchase. Moreover, e-labels allow for labeling to be dynamic in reflecting changes in the product lifecycle or cybersecurity status due to changing risks [STIFEL]. Finally, digital labels with a machine-readable

component can be used by security vendors, tools, auditors, and service providers to automatically assess the vulnerability of software 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 purchase more highly-rated products, even when those products cost more [GOPAVARAM]. Retailers should be engaged as active partners in label delivery.

Addressing Potential Weaknesses

There are potential weaknesses of binary labels with respect to consumer perceptions. 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. 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 INTERACTIVE].

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].

Consumer Education

As a complement to the labeling approach, a robust consumer education program should be developed to increase label recognition and to provide transparency to consumers about important aspects of the labeling program. *Who* provides this information (e.g., labeling program administrator, software providers) will be dependent on the final construct of the labeling program. **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, addressing potential misinterpretations (e.g., false sense of security or dichotomous thinking).
- Technical criteria – what cybersecurity properties are included in the baseline and why and how these were selected
- General information about conformity assessment – how cybersecurity properties are evaluated
- Declaration of conformity – the software's specific declaration of conformity against the baseline criteria, including the date the label was last awarded
- Data Inventory and Protection Attestation descriptions for the software
- 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

- Consumer expectations – how consumers' actions (or inactions) can impact the cybersecurity of a product

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 for those who desire it. 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 in language that is understandable to non-experts, typically written at an 8th grade reading level. 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. 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 INTERACTIVE]. Similar market research for a U.S. population would be informative and should be prioritized.

Note that although this section describes education materials for consumers, education for manufacturers and retailers is also of great importance.

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.

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 1 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 achieve specified goals	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. 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).
Efficiency	**Resources used** in relation to the results achieved	Consumers should be able to quickly gain a broad sense of the product's cybersecurity level without being required to seek out additional information. 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.
	Ease of learning: how fast a consumer who has never seen the label before can accomplish basic tasks	The label should have a minimalistic design and be understandable by those without expertise in cybersecurity or information technology. Since consumers are diverse, there may be those who wish to seek out additional details about the criteria behind the label. Documentation should be described in plain language suitable for most consumers. Those consumers who want more technical detail 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	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 purchase decisions. Consumers should also perceive the label as aesthetically/visually appropriate.

Consumer Testing

To determine a label's appropriateness, selected label designs and consumer education materials should undergo rigorous consumer testing prior to launching a labeling program. Usability testing evaluates the components outlined in Table 1. 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.

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

There is also value in studying – before a program is launched – the *potential* impact of the label on consumers' actual purchase decisions to gauge whether a labeling program actually 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 purchase 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 purchase may differ from actual consumer behavior. Therefore, **periodic testing after program implementation is essential and can include market studies to assess the impact on consumer purchase decisions and the growth of brand recognition over time.**

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

[CSG] National Institute of Standards and Technology (2021) *Cryptographic Standards and Guidelines.* Available at https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines

[CMU] Carnegie Mellon University (2021) *IoT Security and Privacy Label.* Available at https://iotsecurityprivacy.org/

[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.

[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

[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/

[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

[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 INTERACTIVE] 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)

[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

[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

[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, Wą sowicz-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

[NVD] National Institute of Standards and Technology (2021) *National Vulnerability Database*. Available at https://nvd.nist.gov/

[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] National Institute of Standards and Technology (2021) *Secure Software Development Framework*. Available at https://csrc.nist.gov/projects/ssdf

[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/

[VDP] National Institute of Standards and Technology (2021) *Vulnerability Disclosure Guidance*. Available at https://csrc.nist.gov/projects/vdg

[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