Before the
DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, MD 20899

In the Matter of	)
	)
DRAFT Baseline Criteria for Consumer Software Cybersecurity Labeling	))
	)

COMMENTS OF THE CONSUMER TECHNOLOGY ASSOCIATION

The Consumer Technology Association ("CTA")®[1] appreciates the opportunity to provide input to the National Institute of Standards and Technology ("NIST") regarding its white paper, *DRAFT Baseline Criteria for Consumer Software Cybersecurity Labeling* ("White Paper").[2]

I. INTRODUCTION

CTA appreciates NIST's work to enhance consumer awareness about software security, build consensus regarding appropriate cybersecurity criteria and facilitate transparent communication within the software security community. CTA shares NIST's aim to "increas[e] consumer awareness" and "improve the cybersecurity of software" that consumers "purchase and use,"[3] as demonstrated through CTA's participation in organizations like the Council to Secure the Digital Economy, which published the "C2 Consensus on IoT Device Security Baseline

[1] As North America's largest technology trade association, CTA® is the tech sector. Our members are the world's leading innovators—from startups to global brands—helping support more than 18 million American jobs. CTA owns and produces CES®—the most influential tech event on the planet.

[2] NIST White Paper, *DRAFT Baseline Criteria for Consumer Software Cybersecurity Labeling* (Nov. 1, 2021), https://www.nist.gov/system/files/documents/2021/11/01/Draft%20Consumer%20Software%20Labeling.pdf ("White Paper").

[3] *Id.* at 1.

Capabilities"[4] and CTA's active participation and collaboration with NIST on cybersecurity.[5] Adding to our collaborative work with a diverse set of stakeholders, CTA will once again host innovators from around the world at next month's CES 2022.[6] Attendees at CES 2022 will be able to explore products from over 1700 companies working to provide customers with strong security protections and hear from both policymakers and industry leaders on how to enhance cybersecurity going forward.[7]

CTA appreciates NIST's tireless work to enhance software security among consumers as well as its outreach to stakeholders to appropriately define cybersecurity criteria and facilitate an open dialogue within the software security community. In general, CTA agrees with initial feedback from stakeholders regarding development of a consumer label in both the IoT and software labeling contexts.[8] As NIST works to fulfill directives under Section 4(s) of Executive Order 14028 on *Improving the Nation's Cybersecurity* ("E.O."), CTA cautions that a consumer

[4] The Council to Secure the Digital Economy ("CSDE") brings together companies from across the information and communications technology ("ICT") sector to combat increasingly sophisticated and emerging cyber threats through collaborative actions. CSDE is coordinated by USTelecom and CTA. *See* Council to Secure the Digital Economy, https://securingdigitaleconomy.org; CSDE, *C2 Consensus on IoT Device Security Baseline Capabilities* (2019), https://csde.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf ("CSDE IoT C2 Consensus Report").

[5] *See* CTA Comments, *Draft Baseline Security Criteria for Consumer IoT Devices* (Oct. 18, 2021), https://www.nist.gov/system/files/documents/2021/10/29/31-CTA%20Comments%20on%20NIST%20DRAFT%20Baseline%20Security%20Criteria%20for%20Consumer%20IoT%20Devices%20%2810-18-21%29-c3.pdf ("CTA Comments").

[6] Registration is now open for CES 2022 at https://www.ces.tech (last visited Dec. 16, 2021).

[7] *See* CES, "2022 Schedule," https://ces.tech/Schedule.aspx (last visited Dec. 16, 2021).

[8] Namely, that "(1) conveying cybersecurity information to diverse consumers will be challenging; (2) consumers may have difficulty determining appropriate risk levels; (3) a robust consumer education program should accompany the label; (4) consumer testing to assess usability and impact of the label is critical; (5) the label format should be flexible to reflect changing security and label status; and (6) retailers and third-party service providers will play an important role." *See* NIST, *Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward* at 15-16 (Dec. 9, 2021), https://www.nist.gov/system/files/documents/2021/12/03/FINAL_Consumer_IoT_Label_Discussion_Paper_20211202.pdf ("Dec. 9 Stakeholder Discussion").

software label alone cannot solve consumer software security.[9] Rather, consumer software labels can serve as a specialized tool within the greater public-private partnership of ever-improving cybersecurity. As such, the baseline criteria for consumer software labeling must be properly scoped to maximize its effectiveness while recognizing its role in the greater cybersecurity ecosystem. With this awareness in mind, CTA proposes:

- The baseline criteria should define "consumer" to better target the label's intended audience and ensure the label communicates necessary information to maximize comprehension and usefulness.
- NIST should consider methods for communicating technical information of value to subject matter experts and other select stakeholders separately from the consumer label.
- NIST should also avoid duplicating existing labeling schemes, like EnergyGuide or nutrition labels. Instead, NIST should build a scheme based on CTA's key principles and avoid imposing duplicative labeling schemes on companies.
- Whatever software label NIST develops should operate in harmony with the consumer IoT device label directed by the E.O., and neither should require duplicative attestations.

CTA expands on these ideas below and welcomes ongoing engagement with NIST on this important topic.

II. CONSUMER SOFTWARE LABELS MUST REFLECT REALISTIC EXPECTATIONS OF CONSUMER KNOWLEDGE AND KNOWHOW

The baseline criteria for consumer software labels must reflect the real-world knowledge and familiarity of average software end users. To that end, NIST should clarify the distinction between "end user" and consumer so that the criteria leads to a label that meets consumers where they are. To be effective, any consumer label must be tailored to help end-user consumers make purchasing decisions that appropriately consider cybersecurity. NIST should treat more advanced, technical information distinctly from the consumer label so that experts can find and

[9] Exec. Order No. 14028 of May 12, 2021, *Improving the Nation's Cybersecurity*, 86 Fed. Reg. 26633 (May 17, 2021).

utilize the information they need as well. This is best done by focusing the information on the label as "meeting industry standards" in a binary fashion, as NIST contemplates in the White Paper.

A. The Baseline Criteria Should Clarify the Distinction Between "End User" and "Consumer" and Target Labels to End User Consumers

The White Paper should clarify that the "consumer" for whom the software label criteria is designed means an average end user of the software and not intermediary entities that purchase and/or configure software with the intent to place it in the market for end users or security researchers seeking information about a product to assess its security features and practices. Intermediary entities and security researchers often have additional technical knowledge that the average end user of software does not possess. To effectively inform consumers, a label must be designed for an average end user; criteria requiring advanced knowledge is inappropriate for a consumer label.

The White Paper uses "consumer" to sometimes mean individual end users and sometimes entities that purchase software products, which is not always the end user. For example, in Section 1.2 "consumer" appears to refer to individuals and families purchasing software for personal or household use, which uses the term to reasonably describe an average end user of the software.[10] Conversely, a "consumer" described under attestations like 2.3.1.6 Vulnerability Reporting seemingly refers to an entity buying software because the desired outcomes and descriptions require that intended "consumer" to possess technical knowledge.[11]

[10] *See* White Paper at 2-3.

[11] *See e.g.*, *id*. at 7 (stating that the desired outcome of Vulnerability Reporting is that "[t]he 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"); *id*. (stating that "[t]he software provider asserts to reporting vulnerabilities to consumers in a reasonable mechanism either through hosting vulnerability information internally and/or reporting

The "consumer" here is not necessarily an average end user, but rather an intermediary or individual, with advanced technical knowledge, that configures the software and places it in the market for an end user. While these proposed attestations are useful to certain sub-groups (i.e., subject matter experts, security researchers and consumer advocates), they are unlikely to be useful to average end-user consumers and should be addressed separately from the consumer label.

B. To be Effective, Any Communication to Consumers—Including a Label — Must be Clear and Easy to Understand

The White Paper correctly avoids proposing a label with highly technical information or language that would be unfamiliar to most consumers and could provide a false sense of security and/or deter consumers from learning more about software security. The baseline criteria include attestations on software development as well as critical cybersecurity attributes and capabilities (e.g., "software is free from known vulnerabilities") that, if presented on a label, could lead an average end user consumer to believe that the software is unrealistically secure (i.e., "unhackable"). Indeed, the labels should avoid conveying such a false sense of security, and instead convey that the device or software in question was designed to meet certain standards.[12]

C. Software Security Information Intended for Subject Matter Experts Is Inappropriate for a Consumer Label

Ultimately, there are two audiences that should be considered in the Consumer Software Label Pilot program. The first audience is the non-expert consumer; the binary label proposed by NIST presents this consumer with an easy way to determine if the manufacturer has met industry

vulnerabilities to the National Vulnerability Database [NVD] or other appropriate vulnerability repository. The software provider makes it clear how to obtain this information [VDP]").

[12] *See* CTA, "CTA Position Paper on Cybersecurity Labeling, Conformity Assessment and Self-Attestation" (Aug. 17, 2021), https://www.nist.gov/system/files/documents/2021/09/03/CTA%20Position%20Paper%20on%20Cybersecurity%20Label%20Considerations%20Final.pdf ("CTA Position Paper").

standards. The second audience is the "consumer" of the technical information listed in the White Paper. The White Paper should more clearly distinguish between these two target users. The White Paper does appreciate that there are two groups, for example recognizing, "the information needs and wants of a wide range of cybersecurity expert and non-expert consumers", the former including "security vendors, tools, auditors, and service providers".[13] The efforts of experts will improve the overall cybersecurity of the ecosystem, so where a technical element is required as part of the White Paper criteria, the delivery method should be consistent with the intended audience. NIST correctly notes that a binary e-label pointing to a more detailed landing page will serve better than a detailed package label.

Effective communications tailor their message to the audience they serve. The average end user of a software product does not have an advanced degree in computer science to leverage when purchasing software and considering software security. Conversely, enterprise buyers and security researchers will likely find that more detailed descriptions of security practices suit their needs much more than a simple label. Therefore, NIST should clarify that this label will address the needs of consumers as average end users and consider more technically sophisticated communications as a distinct matter.

III. ANY CONSUMER SOFTWARE LABEL SHOULD REFLECT CTA'S KEY PRINCIPLES FOR CYBERSECURITY LABELING

NIST's software label for consumers should build on key principles and avoid copying programs like EnergyGuide or nutrition labels that are designed to convey different types of information. To be most effective, the software consumer label should operate in harmony with NIST's consumer IoT security label.

[13] *See* White Paper at 17-18.

A. NIST's Software Consumer Label Should Build on Key Principles

Analogies between cybersecurity labeling and other existing labeling programs, like those in the energy and food sector, oversimplify cybersecurity.[14] Software security is not a quantifiable value like watts, dollars or percent of daily requirement.[15] Unlike energy ratings and food nutrition values that remain relatively constant year-over-year, a strong cybersecurity practice or measure one year will not necessarily remain "strong" in subsequent years. For instance, creating a password with a prescribed length, combination of special characters and capital letters once constituted a "strong" security measure, but security experts now prefer to incorporate multi-factor authentication on top of passwords. In addition, cybersecurity is not a one-dimensional concept that applies to only one device or use. Any cybersecurity labeling program should be built on risk assessment as much as security capabilities and the labeling system should consider the intended application at the point of design, not all possible uses across all possible sectors.[16] More, a cybersecurity labeling program must remain voluntary and should recognize third party assessments and self-attestations.[17] Self-attestation is necessary to avoid ecosystem overload and should recognize the work of manufacturers who are currently operating via industry best practices.[18]

As described in CTA's position paper submitted in anticipation of NIST's initial labeling workshop, any labeling scheme to address cybersecurity should avoid attempts to copy programs like EnergyGuide, which communicate different types of information on topics with distinct

[14] *See generally* CTA Position Paper.

[15] *See id.* at 2.

[16] *See id.*

[17] *See id*. at 3.

[18] *Id.*

characteristics, and instead build on several key principles.[19] Namely, a cybersecurity labeling scheme should:

1. Be based on industry consensus standards, recognizing that no single standard or set of criteria will be appropriate for all IoT device categories or use cases;
2. Avoid fragmentation in the marketplace through deliberate long-term international coordination;
3. Be built on risk assessment as much as security capabilities, accounting for the intended application of a device at the point of design;
4. Eschew ad-hoc requirements that are not part of regional or international standards;
5. Be tailored to different categories of devices and corresponding risk profiles without implying inferior security for devices that appropriately meet different tiers;
6. Avoid conveying a false sense of security through labels and educational campaigns that clearly convey expectations to consumers;
7. Account for limited space on product packages, including allowing for electronic labeling;
8. Incorporate existing conformity assessment programs into the label's development;
9. Recognize both third party assessment and self-attestation to foster efficiency and avoid overloading the labeling ecosystem; and
10. Accompany a significant consumer education campaign.

Using these key principles as a guide will build a labeling scheme that appropriately accounts for cybersecurity's complexities and allow these practices to evolve over time.

B. NIST's Software Consumer Label Should Operate in Harmony with NIST's Consumer IoT Security Label and Related Standards

NIST should ensure that the software label baseline criteria harmonize with existing and proposed IoT security labels in both the domestic and international marketplaces.[20] Companies

[19] *See* CTA Comments at 4.

[20] *See*, e.g., NIST, *Draft Baseline Security Criteria for Consumer IoT Devices*, (Aug. 31, 2021) https://www.nist.gov/system/files/documents/2021/08/31/IoT%20White%20Paper%20-%20Final%202021-08-31.pdf; *See also* Cyber Security Agency of Singapore, *Cybersecurity Labeling Scheme*, https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls (last visited Dec. 16, 2021).

providing IoT products that also contain software should not have to go through duplicative processes to obtain IoT and security labels. CTA agrees that there is value in establishing brand recognition between marks for consumer IoT and consumer software as well.

Finally, the software labeling system should consider mutual recognition of international marks and labels as they are developed to ensure that the NIST software label sets a baseline equivalent to its international counterparts.[21] NIST can achieve this in part by ensuring that its criteria align where possible with related international standards.[22] A well-defined industry program based on industry developed standards and potentially mapped to NIST criteria has potential to be recognized internationally and presents an opportunity for mutual recognition that the U.S. currently lacks.

[21] *See* CTA Position Paper at 2.

[22] *See e.g.*, ETSI EN 303 645 v2.1.1 (2020-06), "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements," https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf.

IV. CONCLUSION

Building on the considerations above, CTA provides detailed feedback on specific sections of the White Paper in a table below. CTA appreciates the opportunity to provide input. As always, we look forward to continued partnership with NIST to enhance the security of consumer technology products.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

By: *\/s/ J. David Grossman*
J. David Grossman
VP, Regulatory Affairs

\/s/ Mike Bergman
Mike Bergman
VP, Technology and Standards

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7651

December 16, 2021

APPENDIX A: CTA Comments on Baseline Criteria

Section	Topic	NIST Draft Section or Text	CTA proposed comment
Intro	Note for Reviewers	• 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.	A binary label is appropriate and would be consistent with the approach NIST plans to take for the IoT label (as relayed during the Dec. 9 Stakeholder Discussion). However, the label should not cite "the NIST baseline technical criteria." These criteria are a broader articulation of practices which must be translated into industry standards for IoT manufacturers to build to them.
Intro	Note for Reviewers	• Whether additional considerations for the labeling approach, consumer education, or testing are needed – including:	
Intro	Note for Reviewers	o Possible appropriate definitive text for describing the labeling program in consumer education materials.	
Intro	Note for Reviewers	o Best approaches for addressing the needs of non-English speaking consumers.	
Intro	Note for Reviewers	• 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.	Common branding will help reduce consumer confusion. However, note that the August 31, 2021 NIST "DRAFT Baseline Security Criteria for Consumer IoT Devices" ("IoT Draft Baseline") indicates that all "product components" of an IoT device are in scope for that baseline. The IoT Draft Baseline explains that this includes any software or services delivered with the IoT product. A smartphone app would appear to fall under

			both categories. NIST should resolve this discrepancy, preferably without requiring a single piece of software to separately achieve both Consumer IoT and Consumer Software labels.
Intro	Note for Reviewers	• Whether the conformity assessment provisions are appropriate.	
Intro	Note for Reviewers	• Whether a template Declaration of Conformity would be useful for software providers.	
Intro	Note for Reviewers	• Whether more details on evidence required to support assertions would be useful for software providers.	
Intro	Note for Reviewers	• Whether the technical baseline criteria are appropriate, including but not limited to:	
Intro	Note for Reviewers	o The feasibility, clarity, completeness, and appropriateness of attestations.	Please see line-by-line comments in the table below.
Intro	Note for Reviewers	o Normative references to be considered for inclusion.	
Intro	Note for Reviewers	o Potentially requiring that the Software Identifiers attestation take the form of a Software ID Tag.	Standards such as SWID should not be identified so early in the process and NIST's label should remain technologically neutral. SWID, CycloneDX and SPDX are all viable technologies. The ecosystem has not yet caught up to the developing state of SBOM technology. We are encouraged to see continued work to mature SBOM at CISA. However, we recommend waiting before adding SBOM to this baseline.

Sec. 1.2	What is "consumer software"?	*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.*	This appears to be the only definition of "consumer software" in the document. CTA recommends clearly defining "consumer" to mean "average end user."
Sec. 1.2	Goals of the Criteria	Establish a baseline set of technical criteria; Provide criteria for the label; Describe conformity criteria	
Sec. 1.2	Relationship to IoT	These criteria are intended to complement and not to conflict with the IoT Product Criteria which meet the goals of Sec. 4 (t).	
Sec. 1.2	"Minimum" nature	These criteria identify key elements of labeling programs in terms of minimum recommendations and desirable attributes.	
Sec. 2.1	"Attestations"	*"...attestations [are] claims made about the software associated with the label..."*	
Sec. 2.1	Descriptive Attestations	Mfg, device, date, path to support.	
Sec. 2.1	Secure Software Development Attestations	How the software provider adheres to accepted secure software development practices.	
Sec. 2.1	Critical Cybersecurity Attributes and Capability Attestations	Software features resulting from secure SDLC.	
Sec. 2.1	Data Inventory and Protection Attestations	Data that is stored, processed, or transmitted by the software.	

Sec. 2.3	Baseline Criteria (introduction)	*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.* Immediately after, *Several of the criteria address characteristics that may not be included in a specific consumer software product.*	Manufacturers and developers should conform to an industry standard – not to the White Paper. Industry standards provide an important intermediary between objectives articulated in the White Paper and the technical steps necessary to achieve those objectives.
2.3.1.1	Software Provider	"Consumers can quickly and easily determine the author/organization of the software that is making claims."	NIST should revise this provision to meet the needs of consumers, not necessarily subject matter experts in the community who have different needs. NIST should clarify which entities should be considered the "author/organization." Consider a white label software product. This attestation contains "who is making the attestations in the label" and "contact information for an individual within this entity that is responsible for these claims." Assuming JKL Corp is the brand on the product, and XYZ Corp is the developer, which should be the attestation "face"? Presumably reputation and warranty follow JKL, but the technical capability are with XYZ. NIST should also consider how or even if such information would be helpful to consumers. Would a consumer be expected to contact the company directly to inquire

			about cybersecurity issues? The average end user cannot or does not want to advocate for themselves at the necessary technical level. If this provision aims to provide a contact for security researchers to use, it should be reconsidered for use separately from the consumer label.
2.3.1.3	Software Identifiers	“A standardized, unique identifier for each piece of software...Consumers can clearly understand version/build/editions”	NIST should omit this provision. This information is not appropriate for a printed label, as it is often updated. Since a printed label may be a desired approach in some cases, this attestation should not require the identifier per se, but instead should allow for *means to display or locate* the identifier. For example, running software may have a “Help” or “About” option.
2.3.1.5	Software End of Support Date	“A date beyond which the consumer can expect to no longer receive security-related updates” “The software provider asserts the software will continue to receive security-related updates until at least the date specified.”	This is effectively a warranty provision and should not be included in the label. If NIST includes such a provision, it should be for a reference to provisions in the warranty, not stated explicitly here.
2.3.2.1	Implements a Secure Development Process	“a development process that is consistent with the NIST Secure Software Development Framework (SSDF)”	NIST should clarify that manufacturers and developers may use any software development processes that are equivalent to the SSDF by including the following language in this provision: “a development process that is consistent with the NIST Secure Software Development Framework

			(SSDF) **or the equivalent.**" The SSDF should not be the only option. For example, BSA | The Software Alliance has a very well-regarded SDLC framework.
2.3.3.1	Free from Known Vulnerabilities	"as of the assertion date indicated in the label, the software is free from known vulnerabilities"	If NIST includes this provision, it should clarify what constitutes a "known" vulnerability. As written, this attestation could have problematic implications for product liability. For example, if a graduate student posts a vulnerability on his blog, is it "known"? NIST might consider tying this provision to something more concrete, like NIST's Known Vulnerability Database ("NVD").
2.3.3.4	Free from Hard-Coded Secrets	The software does not store secrets utilized for encryption, passwords, or other authentication methods within the software.	
2.3.3.5	Strong Cryptography	"All cryptographic algorithms utilized by the software follow NIST cryptographic standards and guidelines [CSG]."	The wording of this provision should include "or equivalent" to allow for more options. Note that industry best practices often cite NIST standards and guidelines and could be equally applicable to the execution of this provision.
2.3.4.1	Personally Identifiable Information (PII) Data Manifest	"Not Applicable – The software does not store, process, or transmit any PII data."	NIST should refine this language to read: "…or transmit any of the PII data types listed here." Otherwise, the options go from "stores SSN, etc." straight to "no PII", but there are other types of PII that are not on the Supported list.
4	Conformity Assessment Criteria (item 3, "Contents of the	"Any limitations on the validity of the declaration of conformity."	Rather than stating "limitations on the validity," NIST should consider "exceptions to full conformity with the requirements related to the declaration of conformity."

	declaration of conformity”)		
Annex A	Proposed Label Approach	“NIST proposes that a binary label is likely most appropriate”	CTA agrees that a binary label is the most appropriate approach.
Annex A	Proposed Label Approach	“NIST also is proposing coupling the binary label with a layered approach”	
Annex A	Proposed Label Approach	“Physical labels on software packaging should follow applicable labeling standards and be located on a conspicuous, but not intrusive, place”	Physical labels should be an option (assuming an e-label is provided), particularly for small packaging.
Annex A	Proposed Label Approach	“Digital labels (e-labels) (e.g., as described in the ISO/IEC electronic labelling standard [ISO22603]) should be available for all products”	
Annex A	Proposed Label Approach	“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.”	NIST should add “at some point in the future,” since the ecosystem is not fully capable of executing this provision. As written, this provision implies, for example, that scanning a digital label on a product would allow automatic evaluation of whether the software has the HeartBleed vulnerability. This capability may come over time as digital labels, SBOM and vulnerability databases are connected and solutions are deployed with appropriate tools, however it is not available today.
Annex A	Consumer Education	“Consumer expectations – how consumers’ actions (or inactions) can impact the cybersecurity of a product”	NIST should clarify that this provision means that consumers should be educated about the responsibility they share in securing a product.
Table 1	Usability components	<n/a>	NIST should include an additional “Usability Component” as follows:

			Component: “Appropriateness” **Description:** “Ability to help with consumer-level goals” **Consumer Cybersecurity Label Considerations:** “Consumers should not be presented with information that is beyond the average consumer's skill level or which requires significant study to appreciate. Consumer goals should be relatively simple and require no specific cybersecurity technology understanding. Label components should exist to support such consumer goals.” Note that the word “appropriateness” appears immediately following the table, in the introduction to Consumer Testing.