Draft Consumer Software Labeling Criteria

- Submitter’s name: Adetokunbo Salau
- Organization: RiskAide Consulting Inc, Canada

Section	Specific Section	Comment / Suggested Change	Rationale
1.2 Document Scope and Goals (Page 2)	3rd Paragraph *“…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…”*	Consider the following suggested wording change: *“…It also informs the development and use of a label for consumer software which will improve consumers’ awareness, information, and ability to make software selection and use decisions while taking cybersecurity considerations into account…”* Don’t give the appearance that the use of the document is limited to just helping consumers to make a purchase decision. It should be useful for anyone looking to select a software (regardless of whether there is an associated cost to acquiring / licensing the software).	The phrase “purchasing decisions'' (or a variation of the phrase) is used eight (8) times in the document. Each time, the ability for software consumers to make informed ‘purchasing decision’ is cited (or implied) as the basis for establishing the baseline criteria document. Not all potential consumers will require the information on the label for making a buy decision (for example, when looking to acquire a freeware, an open source software or some shareware products). And yet, these software types could still present a level of risk similar to what commercial software exposes consumers to. By putting emphasis on ‘purchased’ software, the document’s scope of applicability could be misconstrued by the document’s audience to be narrower than NIST intended.

Section	Specific Section	Comment / Suggested Change	Rationale
2.3 Baseline Criteria (Page 5)	Subsection 3. Critical Cybersecurity Attributes and Capability Attestations … • Free from Known Vulnerabilities • Free from Hard Corded Secrets	Consider removing the following attestations from under the "Critical Cybersecurity Attributes and Capability Attestations' category: • Free from Known Vulnerabilities • Free from Hard Corded Secrets	"Free from Known Vulnerabilities" and "Free from Hard Corded Secrets" are listed among the Critical Cybersecurity attributes / capabilities. These are neither attributes nor capabilities. They pertain to vulnerabilities and would therefore be better off included in the 'Software Development Attestations' category – since practicing secure Software Development would effectively mitigate these vulnerabilities.
2.3.1. Descriptive Attestation (Page 6)	Subsection 2.3.1.1 Software Provider *"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."*	Consider rewording the statement so that what is being asserted is clear to the intended document audience. Consider following the same convention adopted for the Assertions in the other attestations i.e. *"the Software Provider attests to the…"*	The language used does not help with clarifying what the claim being made is. Also, this language does not conform with the convention followed for the Assertions is the other attestations i.e. "the Software Provider attests to the…"
2.3.1. Descriptive Attestation (Page 6)	Subsection 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."*	Consider including additional guidance / criteria in the draft document to ensure consumers can accurately / clearly distinguish between the descriptions of: (i) software that are in scope of the attestation; and (ii) software that are outside the scope of the attestation but still included in the label.	The label will have two sets of description: ○ Software that are in scope of the attestation; and ○ software that are outside the scope of the attestation but still included in the label. Not establishing the criteria that would compel Software Providers to clearly distinguish between each set of description in the label could lead to consumers becoming confused about which software are in the

Section	**Specific Section**	**Comment / Suggested Change**	**Rationale**
	"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."		scope of the attestation provided by the Software Provider.
2.3.1. Descriptive Attestation (Page 6)	2.3.1.2 Label Scope *"Assertions: The software provider attests to the completeness and correctness of …."*	Consider including relevance as another information attribute that the Software Providers' assertion should address. *"The software provider attests to the completeness, correctness and relevance of …."*	The information provided by the Software Provider, upon which the assertion is being made, may be complete and correct and yet not relevant toward enabling the consumer to make an informed decision regarding the possible selection or use of the software.
2.3.1. Descriptive Attestation (Page 6)	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*	Considering changing the title of this attestation from "Vulnerability Reporting" to "Vulnerability Management" as the latter would more aptly cover all the various subcomponents of the VM process that the rest of the attestation's content seemed to be alluding to.	The main goal / purpose of this Attestation subcategory is not quite clear. The ensuing narratives in the subcategory seem to jump from one idea to another. First, the title seems to suggest that the focus of this attestation subcategory is on 'reporting' vulnerabilities. Then, under the 'Description section', the focus somehow shifts to identifying vulnerabilities. Next, for the 'Desired Outcome' section, the focus once more shifts – this time to 'responding' to vulnerabilities discovered. Finally, in 'Assertions' section, the focus reverts to the initial goal of 'reporting' vulnerabilities.

Section	Specific Section	Comment / Suggested Change	Rationale
	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]…"*		
2.3.1. Descriptive Attestation (Page 6)	2.3.3 Critical Cybersecurity Attributes and Capability Attestations *"Attestation: Free from Known Vulnerabilities"*	Consider providing additional context on what constitutes 'known' vulnerabilities. 'Known' to who or by who? It would be helpful to reference an internationally accepted standard (on the definition of 'known' vulnerabilities).	There is no yardstick that Software Providers and other stakeholders can use to determine / agree on what is deemed 'known' vulnerabilities.
2.3.1. Descriptive Attestation (Page 6)	2.3.3 Critical Cybersecurity Attributes and Capability Attestations *"Description: The provider attests that known vulnerabilities have been fixed.*	Consider rewording this subsection to reflect a more risk-based approach to dealing with vulnerabilities, such as one that is based on potential business impact level or the criticality of business assets underlying the software (versus taking a rigid stance with fixing vulnerabilities).	It is popular among businesses that they follow a risk-based approach in determining what vulnerabilities need to be remediated. *"…that known vulnerabilities have been fixed. "* and *"…It is free from known vulnerabilities…"*. These are absolute statements that Software Providers may be unwilling to make aware that not all vulnerabilities are exploitable

Section	Specific Section	Comment / Suggested Change	Rationale
	Desired Outcome: Consumers should be confident when selecting software that it is free from known vulnerabilities."		and not all exploitable vulnerabilities will result in a magnitude of loss that justifies fixing them Some Software Providers may be reluctant to make this assertion as it could expose them to undue contractual / legal risks.
2.3.1. Descriptive Attestation (Page 6)	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."*	*"Description: The software and all provided updates are cryptographically signed."*	The ending part of the statement in the Description section (as written) gives the impression that the document is advocating for Software Providers to self-sign their certificates. If Software Providers implement self-signed certificates (believing that that is what the document demands), it could lead to a diminishing of the trust that potential consumers would have on the software (as opposed to if the software's certificate was signed by a trusted public CA) having such software.
4. Conformity Assessment Criteria (Page 12)	1st Paragraph: *"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."*	Clarify what the word 'this' in the statement is referring to.	It is not clear what 'this' in the context of the statement is referring to. In order words, what is it that is not a requirement? ○ The option that the software provider's option to use an accredited laboratory or inspection body?; or ○ The Software Provider indicating on the declaration that it is opting to use an accredited laboratory or inspection body?
multiple instances in the document	"Software Developer" used in place of "Software Provider"	Maintain consistency by sticking to just the term "Software Provider" (versus "Software Developer" or "Vendor", etc.) in all places within	A 'Software Developer' (or Vendor) may not necessarily be the software provider or owner and therefore not have ownership / licensing rights to the software (and by

Section	Specific Section	Comment / Suggested Change	Rationale
		the document where the authority to provide the attestation is being assigned.	extension, the authority to issue a legally binding attestation / assertion for the organization).
multiple instances in the document	Various undefined key terms used in the document: consumer software, consumer, attestation, assertion, etc.	Unless terms like “consumer software” “attestation” and “assertion” have a universally understood meaning, it may be beneficial to include a glossary of key terms commonly used in this document.	Doing so will help improve clarity of intent / scope of the document and not leave room for interpretation.