Comments and secretariat observations

Date: December 16, 2021	Document: **Public comments**	Project: NIST cybersecurity document: "Baseline Criteria for Consumer Software Cybersecurity Labelling"

MB/NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
Deloitte & Touche LLP		2.1.3		ed	The document does not contain a reference to what is clearly defined or referenced as a "critical cyber security attribute" and allows interpretation of severity.	Suggest creating a reference table with defined attributes referenced in https://csrc.nist.gov/glossary/term/security_attribute and https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf to ensure continuity.	
Deloitte & Touche LLP		2.3.2.1		ed	The current SSDF referenced is based on self-assigned requirements to comply with the framework. A gap may then exist when insufficient requirements are self-assigned which may avoid the intent of the SSDF.	Suggest clarifying a minimum standard within either the SSDF which includes a clarified intent or creating an appendix which contains a minimal compliance for each practice as it relates to this document.	
Deloitte & Touche LLP		2.3.3.1		ed	"Free from known vulnerabilities" does not currently require scanning or sufficient testing which may allow for ignorance as an excuse.	Suggest creating a table or appendix with the minimal guidelines to be considered "free from known vulnerabilities" including time and expectation such as "conduct annual penetration testing to ensure the application is free from known vulnerabilities."	
Deloitte & Touche LLP		2.3.3.1		ed	"Free from known vulnerabilities" does not require the assessment of risks created by vulnerabilities. It may be impractical to expect.	Suggest changing from "free from known vulnerabilities" to "free from significant risks posed by known vulnerabilities."	
Deloitte & Touche LLP		2.3.3.1		ge	Unknown and zero day vulnerabilities are not mentioned.	Suggest inclusion of a requirement for timely notification and notification method.	

[1] **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial