Comment#	Organization/ Submitter Name (required)	Type*	Section #	Page # (req'd)	Starting Line # (req'd)	Ending Line #	Proposed Change (required)	Comment/Rationale (required)
1		Editorial	2.3	5	n/a	n/a	**Modify**: "Software End of Support Date." **To**: "Software End of Support Date, **if applicable**. "	End of Support date is not applicable for all software (i.e. mobile apps, cloud services). Typically mobile apps and cloud services are supported through the customers service level agreement.
2		Technical	2.3.1	6	n/a	n/a	**Modify**: "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. " **To**: "The name of the software developer/vendor/owner making the claims in the label as well as the **applicable contact information** ~~name and contact information for an individual~~ within this entity that is responsible for these claims is readily available to the consumer."	For large organizations, having an individual listed on a label is not achievable. They have thousands of developers. More appropriate is a contact mechanism a customer can reach out to.
3		Technical	2.3.1.5	7	n/a	n/a	**Modify**: "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." **To**: "Description A date beyond which the consumer can expect to no longer receive security-related updates for any software within the Label Scope **on the operating system versions the software was designated to operate on.** 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 **on the operating system versions the software was designated to operate on.**"	These statements should take into consideration the software itself (i.e. an app) and the OS it's designed to work on (i.e. Android version xxx). As some devices may not be able to get an OS upgrade, these statements should be tied to the current OS.

*Type: E - Editorial, G - General, T - Technical

4		Technical	2.3.1.6	7	n/a	n/a	**Modify**: "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." **To**: "The software provider **asserts to either automatically fixing and updating the software or to reporting** ~~asserts to reporting~~ vulnerabilities **which put consumers at risk** ~~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."	It is necessary to specify that there may be vulnerabilities that do not put consumer data at risk. In these instances, it is better for the customer for it to be automatically fixed.
5		Technical	2.3.2	8	n/a	n/a	**Modify**: "The software provider uses a secure development process that includes all applicable practices contained in the NIST SSDF[SSDF]." **To**: "The software provider uses an **industry recognized** secure development process **(i.e. NIST, etc).** ~~that includes all applicable practices contained in the NIST SSDF[SSDF].~~"	The NIST SSDF is not the only security development process that is well recognized. Adding the general qualifiers of "industry recognized" and "(i.e. NIST, etc)" provides more applicable options software providers.
6		Technical	2.3.3.1	8	n/a	n/a	**Modify**: "Free from Known Vulnerabilities." **To**: "Free from **Publicly** Known Vulnerabilities."	Publicly known indicates its been published and available for everyone to "Know" about.
7		Editorial	2.3.3.2	8	n/a	n/a	**Modify**: "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." **To**: "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 **tampered** ~~tempered~~ with."	Misspelling - "tampered", as-is the word is spelled incorrectly.
8		Technical	2.3.3.5	9	n/a	n/a	**Modify**: "All cryptographic algorithms utilized by the software follow NIST cryptographic standards and guidelines [CSG]. " **To**: "All cryptographic algorithms utilized by the software follow NIST cryptographic standards and guidelines [CSG]**, or are of comparable or better cryptographic strength.** "	NIST cryptographic guidelines are a solid base, but there should be a general qualifier added to be more inclusive and verify that the vendor does not use any NIST deprecated algorithms.
9		Technical	2.3.3.5	9	n/a	n/a	**Modify**: "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." **To**: "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.~~"	Remove the example. The example does not add relevance to the previous sentence.
10		Editorial	2.3.4.1	10	n/a	n/a	**Modify**: "...encrypted when stored or transmitted and if this is done by the software itself or externally." **To**: "...encrypted when stored or transmitted and if this is done by the software itself ~~or externally.~~"	In this context, use of "or externally" is unclear and unnecessary.

11		Technical	2.3.4.1	10	n/a	n/a	**Modify**: "Not Applicable – The software does not store, process, or transmit any PII data." **To**: "Not Applicable – The software does not store, process, or transmit any PII data **of the types listed above.**"	Designating "of the types listed above" defines the scope appropriately
12		Technical	2.3.4.2	10	n/a	n/a	**Modify**: "The software does not store, process, or transmit any Location Data." **To**: "The software **provider** does not store, process, or transmit any Location Data."	Add "provider" to be consistent with previous language.
13		Technical	3.1	11	n/a	n/a	**Modify**: "The software provider is using a label that has undergone rigorous consumer testing to ensure its usability." **To**: "The software provider **includes a standardized** label **to acknowledge that the software** has undergone rigorous consumer testing to ensure its usability."	The current statement identifies only the "label" has gone through consumer testing, not the software itself.
14		Technical	4	13	n/a	n/a	**Modify**: "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" **To**: "Signature of authorized individual acting on behalf of the software provider including **applicable contact information** ~~name and title~~ as defined in Section 2.3 Baseline Criteria, Clause 2.3.1.1 Software Provider"	For large organizations, having an individual's name and title listed on a label is not achievable as they could change positions and responsibilities after submitting the assertion. They have thousands of developers. More appropriate is a contact mechanism a customer can reach out to.