NIST colleagues,

Thanks for the opportunity to review *Draft Baseline Criteria for Consumer Software Cybersecurity Labeling*. The following summarizes our thoughts ten aspects of the Criteria, in the order posed in the Note for Reviewers:

1. The criteria are likely to moderately improve consumer software security awareness and actual software cybersecurity.
2. Ethical software providers are likely to invest in baseline conformance and supply truthful attestations, resulting in modest cybersecurity improvements.
3. Label-specific criteria are reasonably appropriate and should be effective for a motivated, educated segment of consumers who care about cybersecurity.
4. The label should include a simple, clear, jargon-free descriptive statement about its overall meaning. Keep in mind most consumers don't know what NIST is.
5. Consumer education is essential to the project's success, and should include testing of both educational materials and the labeling itself.
6. The software and IOT binary labels should be very similar in appearance.
7. In an ideal world conformity would be verified via independent audit, but we understand self-attestation is a more affordable & practical approach for now.
8. A template and examples would help software providers create useful, consistent Declarations.
9. Other than the 3 manifests, there don't appear to be any evidentiary requirements since all other Assertions take the form of self-attestation.
10. The baseline criteria are generally appropriate. Software identifiers should follow some standard format for consistency and readability.

An additional comment:
It's unclear how the proposed labeling methodology will adapt to future revisions to the baseline. As new Criteria are added in future years, there will inevitably be new versions of the baseline. The label should indicate which version of the baseline a software product conforms to (e.g., "2022").

Sincerely,
Michael McCormick, CISSP
Founder & President
Taproot Security LLC
Web: www.taprootsecurity.com
Blog: www.ntkblog.org
Facebook: https://www.facebook.com/taprootsec
Twitter: https://twitter.com/taprootsec