Below are my comments on the draft

2.1. Methodology

2.1.2. Secure software development attestations.
This category should also identify which of the "accepted secure software development practices" this specific version of software adheres to. The reason is these practices are acceptable at a given date; they will evolve with time.
"2.3.2.1. Implements a Secure Development Process" mentions NIST SSDF, but, as the title of section 2.3 states, this is the baseline. One should expect software developers to also comply to other practices, which should also be mentioned.

2.3.3.5 Strong Cryptography

A reminder to the consumer that the cryptography was strong at the time listed in "2.3.1.4 Attestation Date" should be helpful.

2.3.4.1 Personally Identifiable Information (PII) Data Manifest

The PII list shown is but a subset of what GDPR defines as personal data. LGDP and APPI are not far behind. We should assume companies who want to use this labeling criteria may want to sell their products in the EU/EEA, Brazil, and Japan (to name a few). I propose the Assertion should either outline which PII/personal data it is being used, and maybe also mention which definition of personal data it uses. After all saying "this software does not store, process or transmit any PII data" when it handles email addresses and associated IPs would cause headaches in countries with more restrictive privacy policies than the US.

2.3.4.2 Location Data Manifest

My concerns presented in 2.3.4.1 also apply here.

3.2 Layered Approach

The customer should be able to freely obtain a means to scan this label and read its contents. This will probably be done using some kind of software/app that is available through the website the government is expected to curate information on this labeling program.

This label should also provide enough info so customer at a glance can identify the main points of the attestation:
- Does it use PII? (2.3.4)
- Date (already mentioned in 3.1)
- Secure? (2.3.3)

Appendix A, Proposed Label Approach

A binary label with just one "seal of approval" is draconian. For instance, what would a binary seal say about PII data in a medical app? Also, it should not require understanding of a language, so it needs to

be more graphic/iconic. Instead of colours, it should use an arrow length as a B&W version of the EU energy efficiency letter grade. Finally, it should account for blind customers.

--
Another vibrant ASCII production