First, I'd like to say that this is a great draft and includes many elements which make it so in this important area. Note that while I'm providing comments as an individual, I'm doing so as an expert in Applications Security, Software Assurance and Secure Development, as I was the founder and leader of the secure development program for the largest technology company in the world at that time (HP, before it split off into smaller companies), and have spent decades leading secure development activities across multiple corporations and have co-invented a secure development (specifically security requirements gap analysis and threat modeling) methodology taught to hundreds of people and used in multiple large corporations.

Regarding the specific questions on which you asked for feedback, below are my responses on the ones on which I have feedback:

- Whether criteria will achieve the goals of the EO by increasing consumer awareness and information and will help to improve the cybersecurity of software which they purchase and use.

  There are a few risks to it achieving the goals:

  1. Optional binary labeling schemes risk lack of adoption, and thus goal achievement. For labeling to achieve the EO goals, mandatory negative labeling (meaning labeling of lack of attestation of label criteria) may become required at some point, potentially via FTC false or misleading advertising authority under the FTC Act - as lack of testing and attestation has a very high probability of not meeting advertised claims. The potential weaknesses section should address adoption risk as a potential weakness and have an explicit plan on how to address.

  2. While the binary nature of the label has merit, developers may take liberties with ambiguities in assertion wording to make unwarranted attestations in order to obtain the label. Rigorous disambiguation of assertion wording in the criteria is required to minimize this risk. I've included an example in my comments below, but I'd recommend a careful review of each assertion for any possible ambiguities and rewording as necessary to disambiguate.

- Whether the criteria will enable and encourage software providers to improve the cybersecurity aspects of their products and the information they make available to consumers.

  Only if the labeling schemes gain traction, such that they become an economic buyers signal. Otherwise, this will all be for naught. Thus the importance of addressing adoption risk as a potential weakness with a plan to address.

- Whether the labeling-specific criteria are appropriate and likely to be effective for consumers.

  Yes, but see specific feedback below on particular criteria. I like the simplicity for consumers of the binary layered label.

- Whether a single, overarching statement that the software product meets the NIST baseline technical criteria should be included on a label, or whether alternative statements would be appropriate.

  As to the statement, yes, a concise statement of above should be included.

  It's unclear whether a binary label will work in that most software developers may have trouble meeting all the baseline criteria, and if they can't get partial credit, and have the market encourage increased levels (for instance a 5-star rating), the rating may not gain sufficient traction to matter. If so, switching to a tiered rating may be required. I prefer the current baseline criteria and a binary rating, but not sure how many software providers would be willing and able to meet it fully from the start, rather than building up to it incrementally via a tiered label.

- Whether the software label approach and design should be unique or extended to the IoT product label (also directed in the EO) to facilitate brand recognition, even though the technical criteria will be different.

  I recommend extending not only the label approach and design, but *also* applying at least some of the software label criteria to IoT product label criteria - especially the Software Development Attestations, since IoT contains software (even embedded firmware is a form of software) and the IoT software should thus meet the baseline software label criteria.

- Whether more details on evidence required to support assertions would be useful for software providers.

  Yes. It would help disambiguate, and reduce the risk of intentional or accidental unjustified attestations.

- Whether the technical baseline criteria are appropriate, including but not limited to:

  Regarding 2.3.2.1 Implements a Secure Development Process clarity, the attestation will need to define "applicable" to avoid abuse of the ambiguity. For instance: "applicable meaning that for a practice assessing a type of artifact, if the artifact (e.g. source code, architecture, etc) is an element of the software, the practice is applicable." Without a rigorous definition of applicable, software providers will be incented to declare numerous practices as non-applicable to avoid having to admit that they don't do them when they should.

  Regarding 2.3.2.1 feasibility, note that 100% of applicable SSDR practices might be too high a bar for the initial binary label (though I agree that the SSDR practices are appropriate). If NIST finds it necessary to relax requiring all applicable SSDR practices, a minimal criteria for the binary label might be the practices required in NISTIR 8397 (Guidelines on Minimum Standards for Developer Verification of Software), with additional SSDR practices being incorporated into a tiered (e.g. 5 star) label. Regarding completeness, alternatively, an additional Software Development Attestation for section 2.3.2 could be NISTIR 8397 conformance.

I’d like to applaud the use of “baseline of due diligence” in the introduction. My hope is that the labeling criteria and subsequent traction of it could also provide the basis for a professional due diligence standard, suitable for liability or even malpractice determination, which is another significant market influence which could further the goals of the EO. Do not let anyone convince NIST to remove the “baseline of due diligence”! NIST is in an ideal position to establish a due diligence baseline in this area.

I’d also like to comment on an asserted weakness of voluntary cybersecurity labeling: “dichotomous thinking” - in large part, I disagree that this is a weakness in practice. In fact, such thinking is in large part correct. In our experience performing hundreds of security assessments, we uniformly found that unassessed systems are insecure (are riddled with undiscovered vulnerabilities and/or security weaknesses). So, while a label certainly doesn’t assert absolute security, it is roughly accurate that once the label program has a modicum of traction, that labeled software is in fact more secure than unlabeled software in most cases. Reasons include that failure to assess security (lack of robust secure development process, such as required by 2.3.2.1) means the software will be riddled with vulnerabilities. Secure development process will result in a far higher degree of assurance of secure software in comparison. So, that only leaves software that implements 2.3.2.1 but lacks a label. While for a short period of time, there will be cases where secure development processes are implemented without labels present, the failure to invest in labeling is itself an indicator of lack of prioritization of security, so even then, existence of a robust label (such as the baseline criteria) is a good proxy for being more secure than unlabeled software. And even to the degree that it is inaccurate in some remaining cases, the market incentive to do the work to be able attest to the label criteria is beneficial in achieving the EO goals. Therefore, I would advise against consumer education warning against “dichotomous thinking” and rather treat the small inaccuracy it represents as a side benefit of the labeling program, as it is a reasonable approximation, and generates desirable market incentives to make the label an effective market signal.

Thanks for seeking comments, and great job on the draft!

John Diamant, CSSLP, CISSP