Cybersecurity Coalition

Cybersecurity Coalition Comments to NIST on Consumer Software Labeling Baseline Criteria

Thank you for the opportunity to provide feedback on the *Draft Baseline Criteria for Consumer Software Labeling*.

Baseline Criteria. Aside from the specific feedback below, we find the baseline criteria put forth in Section 2 are appropriate and applicable to a wide range of consumer software use cases. That being said NIST can consider to focus the label on end-use consumer software, and consider the alignment of the approach with the IoT label as proposed. As the baseline criteria are likely to evolve over time, we encourage NIST to ensure that flexibility is maintained as different product areas are likely to need different criteria and/or approaches, as well consistency with industry and international standards (which evolve as well).

- We encourage NIST to remove or alter Section 2.3.3 *Free from Known Vulnerabilities*. We do not believe that this is feasible in many circumstances and could create a false sense of security for the consumer. Software vulnerabilities are discovered at rapid rate and the likelihood that vulnerabilities could become known after the label is generated is highly likely. In the case of digital software, this would result in a nearly constant updating conformity to the requirement that could see a label present one day and gone the next. For physical software, the label would likely be non-compliant shortly after the label is applied to the box.

  Additionally, there is no specification of what vulnerability are considered in scope. For example, the presence of many known "low" vulnerabilities in Application A is significantly different than the presence of even one "high" or "critical" vulnerability in Application B. And yet, under the proposed criteria, both could be considered non-compliant with the criteria, even though the risk to the consumer is likely negligible to none with Application A.

  As an alternative to removal, the criteria should require an attestation that the software producer has a process for identifying and addressing known vulnerabilities through the product lifecycle. This could be done as part of, or consistent with, Section *2.3.1.6 Vulnerability Reporting* and/or Section *2.3.2.1 Implements a Secure Development Process, and implementation of Security Update capabilities.*

One options could be something like this:

> 2.3.3.1 – Known critical and high vulnerabilities are mitigated at the time displayed on the label.
>
> Description: The provider attests that known critical and high vulnerabilities have been mitigated prior to the time displayed on the label.
>
> Desired Outcome: Consumers should be confident when selecting software that known critical and high vulnerabilities have been addressed by the time displayed on the label.
>
> Assertions: The software provider asserts in good faith that as of the assertion date indicated on the label, the software is free from known critical and high vulnerabilities.

- We find that Section *2.3.4 Data Inventory and Protection Attestations* is overly detailed and possibly out of scope. For example, the concept of personally identifiable information (PII) clearly varies from one country to the next and in most cases is enumerated and protected by some form of regulatory mechanism that requires appropriate protections. Additionally, these criteria contemplate issues involved with data privacy which is not called for within the Executive order. We encourage to NIST to consider updating this entire section to be a single criterion:

> 2.3.4 Data Inventory and Protection
>
> Attestation: Data Inventory and Protection
>
> Description: Some types of software collect data about users of the software as part of its normal operation. The label addresses what data is being collected from or about the user and indicates how that information is safeguarded.
>
> Desired Outcome: Consumers should clearly understand what data is collected and stored by the software and how the data is safeguarded.
>
> Assertions: The software provider makes the following assertions:
>
> - The software collects and stores the following data: [enumerated data types]
> - The software safeguards this information in the following manner: [enumerated list] of safeguard mechanisms]

Label Format and Content. The "label" concept centers on transparency and effective communication of information to consumers prior to purchase and could include many forms of communication, not just a physical sticker on a physical product. We feel that NIST's proposed approach of a using a binary top-level label, combined with a one or more additional layers available to interested consumers, is consistent with our views and previous feedback. The relative simplicity of a binary label combined with access to more detailed, use case specific information, ensures that various types of consumers will be able to effectively use the label. Consistency between label-approaches (e.g. with industry and international schemes) used would also be key to avoid fragmentation and consumer confusion.

Consumer Usability and Testing. We agree that a robust effort to generate and maintain consumer awareness and education concerning security labels will be essential to long-term success. To that end, the Coalition strongly agrees that more data collection and research is necessary to understand what constitutes an effective label from a consumer perspective. This research and testing must inform and wide-spread and sustained education campaign via public-private partnerships. EO 14028 requires pilot programs for both software security labeling and IoT security labeling for consumers. While secure software development practicesand baseline IoT cybersecurity capabilities have differing criteria, we urge NIST to continue examining ways to combine the two efforts so that the security label can apply to both consumer IoT devices and consumer software,[1] leveraging the foundational consensus on definitions achieved in the 8259 series, and 8259A. Presenting different security labels for multiple products may undermine consumer engagement and understanding.

[1] In the future, NIST can consider adding technical criteria relevant to hardware capabilities that harden software security protections as appropriate such as secure boot, secure execution, secure device on-boarding (to the extend there is relation to IoT), trusted-execution environments, and the use of hardware root-of-trust – this would be more relevant for the IoT and software harmonized approach.