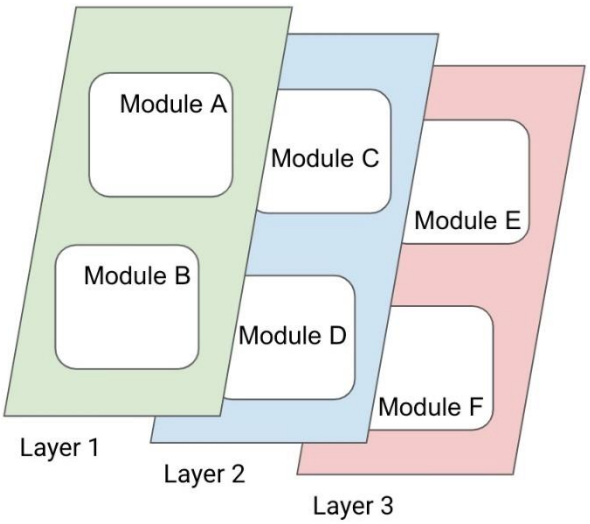
Cybersecurity Coalition

Cybersecurity Coalition Comments to NIST on Consumer Software Labeling

Thank you for the opportunity to provide suggestions for the consumer software labeling effort required by Executive Order (EO) 14028.

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. The format and content should be adapted for the context in which the consumer is considering purchase of the product. As such, we encourage NIST to explore a layered and modular approach to the label, while supporting E-labeling concepts. Layers can reflect increasingly detailed security information, and for the purpose of the pilot, can start with the highest-level risk to consumer security and information asymmetry (e.g. Consumer IoT). Subsequent layers may be hosted elsewhere (such as a product information webpage via a link or QR code), providing information on the underlying security framework and conformity process, and finally providing additional technical data and machine-readable capabilities.



- **Layer 1:** Consumer-facing layer focused on high level, actionable information for consumers. *Module A* could include a standard symbol or phrase indicating participation in the labeling program. *Module* B could include flexible, risk-based information from the vendor regarding the most critical security features or capabilities for that product, in alignment with the security framework to which the product conforms (see "standards compatibility, below). This layer also includes a pathway (i.e., link, QR code, etc.) to the second layer.
- **Layer 2:** More detailed information hosted elsewhere, such as on a vendor product page. *Module C* could include the specific security standard to which the finished product conforms (i.e., NIST Secure Software Development Framework, CTA 2088 or EN 303-645 for Consumer IoT, ISO/IEC standards). *Module D* could include standard language reminding users of the limitations of the label and that users must still take steps to ensure security. This layer also links to the third layer.
- **Layer 3:** Highly detailed information, including data for automated consumption. *Module E* could include information regarding the conformity assessment process and other relevant items chosen by the vendor. *Module F* could include actionable data in a machine-readable format that can rapidly convey security information at greater scale, such as structured formats for an SBOM.

Limitations and Risks. A label should not convey a false sense of security. Label information may not keep pace with the changing prevalence of vulnerabilities, threats, and defensive technologies related to the labeled software, nor does it provide a complete picture of the security posture of the manufacturer. Consumers need to understand the role they play in securing the software and the environment in which it operates, even though this information

may not be included in a label. If consumers do not understand what the label is and is not conveying, they may not take appropriate security steps, such as updating their software or using strong passwords. In addition, if consumers are presented with too much information or too many labels, it can impede consumers' ability to make informed decisions.

Usefulness. The security label should be developed to achieve the specific purpose of helping purchasers of software make informed choices based on security information communicated through the label. In the context of consumer IoT labeling, some survey data suggests that consumers are concerned about the security of smart devices, could find a label communicating security information helpful, and could change purchasing behavior based on the label content. However, there is a lack of definitive information on exactly how consumers would make use of a security label nor reliable data on how consumers value 'security' over other features in the device. The pilot program should aim to collect information regarding the impact of a security label on IoT consumer decision-making in live settings. In addition, we recommend that success metrics for a labeling pilot program include whether the label is readily understood by consumers, presents the most salient security information for consumers, and is actionable for consumer purchase decisions.

Standards Compatibility. Software vendors may use a variety of credible secure development frameworks, some of which require substantial investment for compliance. These may include the NIST Secure Software Development Framework, the OWASP Software Assurance Maturity Model, Common Criteria (ISO/IEC Standard 15408), the BSA Secure Software Framework and the SAFECode Fundamental Practices. We recommend that any labeling program recognize conformity with these and other established international standards and best practices, building upon existing efforts. Given the diversity of consumer software and devices, vendors should be empowered to choose the most critical security information to present to the consumer, as long as it is mapped to the internationally accepted security framework to which the vendor is attesting conformity. However, only those standards and best practices accredited or recognized by NIST or other widely acceptable authority (which may include, e.g., a private sector body) should be eligible for inclusion in the label program, to avoid inclusion of weak, non-credible, or irrelevant frameworks that may undermine trust in the label.

Conformity Assessment. To streamline participation and align with current industry practices, we recommend that any labeling program recognize multiple vendor conformity assessment approaches, including self-attestation and third-party assessments with standards and best practices. However, as noted above, the declaration of conformity must relate to a specific, internationally recognized standard or framework, and it must be understood by label program participants that false or misleading declarations may constitute an unfair or deceptive practice under Sec. 5 of the FTC Act. Further, conformity assessment programs must support mutual recognition to reduce the compliance burden on software producers.

Alignment and Consistency. EO 14028 requires pilot programs for both software security labeling and IoT security labeling for consumers. While secure software development practices and baseline IoT cybersecurity capabilities have differing criteria, we urge NIST to consider ways to combine the two efforts so that the security label can apply to both consumer IoT devices and consumer software, 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.