# Executive Order – NIST Workshop position paper

(Consumer software labeling)

Microsoft Corporation

## Introduction

Microsoft significantly invests in secure software development activities, and we support efforts to provide software consumers with greater awareness of and transparency into the security practices of their software providers. One way to potentially increase awareness and transparency is through a consumer labeling program. While consumer software labeling poses conceptual and operational challenges, such as the need to scale and to ensure consumers understand the limitations of labels themselves and what they can convey, an effective approach to labels should help consumers make more informed procurement choices.

A consumer software label should be easy to understand and communicate a clear value proposition, but doing so consistently across vast, complex, and dynamic software categories will be challenging. Among well-known consumer labels in other contexts, we anticipate a software label may be more akin to a nutrition label, which benefits from more nuanced consumer interpretation, than an ENERGY STAR label, which conveys straightforward information about energy use. Just as nutrition decisions are one component of a consumer's efforts to achieve positive health outcomes, in the context of software, broader circumstances, including user practices, also impact security risk. Conveying that a label does not equate to secure use of a product should be a core consumer awareness objective.

There are also key distinctions to consider. Unlike food products, modern software is continuously updated, posing further challenges to making labels that reflect a point-in-time evaluation meaningful over the life of a software product. Other variables include different update processes and varied commitments to product support among providers. Moreover, threat actor activity will impact risk and adds another dimension to software labeling challenges. While a tiered labeling scheme may offer more context for consumer choice, it may also create incentives for threat actors, with a lower-tier label signaling a gap or weakness in practices.

## Scope

Given conceptual and operational challenges, we encourage NIST to narrowly scope a pilot program and apply lessons learned as the scope broadens. Understanding circumstances in which consumers might encounter a label, how those circumstances impact consumer choice, how consumers interpret or understand labels, and how consumer software and IoT labels will interact could influence initial scope decisions. For example, consumers may encounter labels for applications in an online marketplace differently than they encounter labels for software that is pre-loaded to a device when it is purchased. If integration with the proposed consumer IoT labeling program would benefit a labeling approach for pre-loaded software on a device, then applications in an online marketplace could be a better initial target. NIST could also partner with app stores to scale a consistent approach to helping consumers find and learn more information about the significance of a label. For our Microsoft Store, we would welcome the opportunity to explore approaches with NIST.

We also encourage NIST to consider how to clearly identify the object being labeled, especially given that labels may apply to applications with various back-end configurations and that leverage cloud services (for example, a cloud-based email client). A consumer could also configure a software client to use multiple services that the original software provider did not develop. Given that labeling software with configurable back-end services may require greater coordination across client software developers and service providers to represent the full scope of dependencies in an end product, NIST could scope an initial pilot narrowly and phase expansion over time.

## Labeling Criteria

A labeling program could also phase its approach to criteria to achieve the goals of EO 14028, maximize value to the consumer, and scale over time. For an initial phase, labels attesting to secure development practices at the publisher level would provide efficiencies. In addition, a label could describe lifecycle support policies. Support planning and transparency are recognized security principles and features in several security standards and policies, such as NISTIR 8259 and the UK's proposed consumer smart product security regulation. For subsequent phases as the program matures, NIST could assess how to integrate specific, high-impact security properties into labels, such as "enables multi-factor authentication" and "encrypts data at rest and in transit."

Based on our experience with Microsoft's Security Development Lifecycle (SDL), the developer tools and services that we provide, and our participation in various industry security initiatives (such as SAFECode), we recommend that labeling criteria for secure software development practices focus on an outcomes- or process-based framework rather than specific, prescriptive technical controls, maintaining flexibility, allowing for applicability to diverse industries, and supporting innovation. We propose aligning labeling criteria with existing standards, best practices, and tools, such as ISO 27001 (Annex A.14), ISO 27034, NIST's Secure Software Development Framework, and SAFECode's Fundamental Practices for Secure Software Development (3rd Edition). The ongoing implementation of EO 14028 will result in key references for attestation artifacts and evidence as well.

## Open-Source Considerations

Open-source security is a key consideration for consumer software labeling criteria. Most software products include some open-source code, but because open-source developers will not often be the entities seeking a label for a finished product, there may be few incentives for them to follow labeling criteria. However, managing the risks of including third-party components is a typical feature of a secure development framework, and open-source repositories and development tool vendors can provide tooling and guidance to support secure development practices that help developers keep dependencies updated. These include automated vulnerability scanning and remediation tools that demonstrably reduce the time it takes to remediate vulnerabilities versus manual remediation. Source code repositories on GitHub, and industry initiatives like OpenSSF, already provide information about code security, such as through the OpenSSF Scorecard and CII Best Practices Badge Program. Scores and badges can indicate increasing levels of testing or assessment, such as if code has been processed using an automated scanning or remediation tool, to help developers make informed decisions and pursue further testing if needed. We encourage NIST to work with these industry initiatives to align and validate labeling criteria with automated testing capabilities to support developers seeking a label or to demonstrate use of practices consistent with what a label requires.

## Conclusion

A label must not only clearly communicate to consumers the security value of choosing a conforming product but also that their individual configurations and other user decisions will affect their risk posture. NIST could consider a phased approach to scoping a consumer software labeling program, beginning with less configurable software and expanding to software with back-end services from multiple providers, as it creates more mechanisms for collaboration on attestation over time. NIST could also consider how to strengthen user understanding of what is being communicated through labels during a pilot. Software marketplaces like app stores could be key partners in providing information to consumers about label meaning and interpretation. Consumer awareness could also result from incentivizing consumer use as well as encouraging industry participation, including by leveraging existing security compliance artifacts and taking other steps to achieve efficiencies. Obtaining relevant security certifications and authorization, such as ISO 27001 and FedRAMP, could be sufficient to meet labeling criteria or otherwise streamline processes. Additionally, EO 14028 implementation activities might result in criteria and conformance demonstration methods to which a label could align, enabling consumers to benefit from security investments already being made by federal software providers.