August 17, 2021

Kevin Stine
Chief Cybersecurity Advisor and Chief, Applied Cybersecurity Division
National Institute of Standards and Technology
100 Bureau Drive, Gaithersburg, MD 20899

Via email to labeling-eo@nist.gov

Dear Mr. Stine:

BSA | The Software Alliance[1] appreciates the opportunity to provide this submission in response to National Institute of Standards and Technology's (NIST) call for papers on consumer software labeling.[2]

BSA is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, providing the products and services that power other businesses. BSA members are also leaders in security, having pioneered many of the software security best practices used throughout the industry today.

BSA supports the goal of the Executive Order on Improving the Nation's Cybersecurity (EO), which generally focuses on improving the cybersecurity of the Federal Government. BSA appreciates the importance of identifying and promoting "secure software development practices or criteria" and has, in fact, helped compile those practices as one component of the BSA Framework for Secure Software,[3] the proposed labeling program runs the risk of providing consumers a false sense of security and impression that cybersecurity is static, as well as a justification to ignore the important role they play in cybersecurity.

As a preliminary matter, pursuant to the scope of the EO, it is important for NIST to ensure that the proposed consumer software labeling scheme does not have unintended consequences for enterprise software. Against this backdrop, the EO tasks NIST and the Federal Trade Commission (FTC) with identifying secure software development practices or criteria for a proposed consumer software labeling scheme. The first part of this effort, identifying secure software development practices, is achievable as industry has been working on and implementing these practices for years. However, BSA is concerned about the unintended consequences of the proposed consumer software labeling scheme.

1. Secure Software Development Practices

BSA published the BSA Framework for Secure Software, a risk-based, outcome-focused, flexible framework for, among other uses, communicating between stakeholders about software security risks. The BSA Framework for Secure Software identifies the three functions for secure software: (1) Secure Development, (2) Secure Capabilities, and (2) Secure Lifecycle. Within these functions, the BSA Framework for Secure Software includes "diagnostic statements" that are useful to organizations as they improve their software security as well as to the task at hand. For example, within the Secure Development function, there is a diagnostic statement "Compensating controls are identified and mapped to

[1] BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, CNC/Mastercam, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Workday, and Zoom.
[2] NIST Workshop and Call for Papers on Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software, available at https://www. nist.gov/itl/executive-order-improving-nations-cybersecurity/workshop-and-call-papers-cybersecurity-labeling.
[3] The BSA Framework for Secure Software, available at https://bsa_software_security_framework_web_final.pdf.

20 F Street, NW, Suite 800 P 202-872-5500
Washington, DC 20001 W bsa.org

threats." NIST and the broader community will find such a diagnostic statement helpful as we identify specific secure software development practices.

Notably, the BSA Framework for Secure Software is mapped to the NIST Secure Software Development Framework and international standards and references other frequently cited resources like SAFECode's Fundamental Practices for Secure Software Development.[4]

2. A Consumer Software Labeling Program

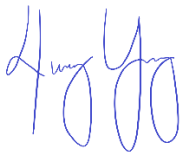
Any label communicates information from a point in time. Software, of course, is not a static deliverable. Software is deployed in a complex environment, that is, an environment with diverse, connected, interdependent, and dynamic actors. Additionally, modern software evolves as it is updated. Given these facts, it is nearly impossible for a label to accurately communicate to a consumer that the software included is "secure" as of the date of the label, and it is almost guaranteed to be obsolete as adversaries advance their tactics, techniques, and procedures. Accordingly, security is best understood as part of an ongoing and iterative process rather than a snapshot in time.

In the discussion on cybersecurity labeling, one frequent model identified is Energy Star. However, Energy Star is not a good model for consumer software security. Measuring energy efficiency ("using less energy to get the same job done"[5]) is object and static. When a laboratory determines that a television "consumes three watts or less when switched off,"[6] that television consumes three watts or less when switched off today and tomorrow. In contrast, a label that proclaims consumer software is secure cannot possibly be expected to be accurate in the future because the consumer software is subject to a complex ecosystem, for example its security will be impacted by actors who actively seek to undermine its security, user who fail to update it, and to the effects of governments holding (or not holding) hackers or their state sponsors accountable. And, as demonstrated in BSA's Framework for Secure Software, software development practices constitute only one of several important functions the are comprised in the software's security.

Unfortunately, the consequence of a label communicating consumer software is "secure" at a point in time is that it will likely give consumers a false sense of security and may decrease the likelihood that consumers take reasonable steps to protect themselves—steps that might take if they were not told that the product is secure. Because a label may undermine the purpose of the EO, a purpose BSA supports, BSA recommends NIST proceed with caution.

Thank you for the opportunity to provide this submission and for your consideration of our views. BSA looks forward to working with NIST on this important effort.

Sincerely,



Henry Young
Director, Policy

[4] SAFECode Fundamental Practices for Secure Software Development, available https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf.
[5] What is Energy Efficiency? available at https://www.energystar.gov/about/about_energy_efficiency.
[6] What Makes a Product ENERGY STAR? available at https://www.energystar.gov/products/what_makes_product_energy_star#:~:text=ENERGY%20STAR%20products%20are%20the%20same%20or%20better,Protection%20Agency%20or%20the%20US%20Department%20of%20Energy.