The Software Alliance

BSA

November 5, 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 ssdf@nist.gov

Dear Mr. Stine:

BSA | The Software Alliance[1] appreciates the opportunity to provide the below comments to the National Institute of Standards and Technology's (NIST) Secure Software Development Framework Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities (SSDF).

BSA is the leading advocate for the global enterprise 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 governments and businesses. BSA members are also leaders in software security, having pioneered many of the software security best practices used throughout the industry today, including The BSA Framework for Secure Software.

As noted in Strengthening Trust, Safeguarding Digital Transformation: BSA's Cybersecurity Agenda, robust software security is one of BSA's top priorities and BSA specifically supports "[u]sing public-private partnerships to design laws and policies that improve software cybersecurity risk management rather than only creating a compliance mindset and accompanying checklists." To that end, BSA applauds both this process and the numerous references within the SSDF to The BSA Framework for Secure Software, as well as other best practices and international standards.

As a preliminary matter, improving the security of software requires more than securing the development of that software, though secure development itself is both a significant challenge and an important goal. In addition to secure development, improving the security of software requires software have secure capabilities and a secure lifecycle. To further the improvement

[1] BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, CNC/Mastercam, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

of secure capabilities and a secure lifecycle, BSA recommends NIST direct organizations that develop software (both in the public and private sectors) to The BSA Framework for Secure Software, which provides a risk-based, outcome-focused, flexible framework for achieving these additional goals.

Section 4(e) of the Executive Order on Improving the Nation's Cybersecurity (EO) directs NIST to "issue guidance in identifying practices that enhance the security of the software supply chain" which "shall include standards, procedures, or criteria" regarding ten identified activities.[2] To accomplish this task, NIST has mapped the ten activities in Section 4(e) of the EO to SSDF practices in Appendix A of the SSDF.

While each of the practices and tasks, if well-implemented, would benefit or improve software security, BSA is concerned that there is insufficient consideration of the costs of each practice or task. Consequently, in a given scenario, software developers could deliver to US Government customers a more secure software product or service using scenario-specific considerations but instead will be required to complete specific tasks. Greater focus on risk-management and corresponding flexibility will allow software developers to meet an agency's requirements in more cost effective and innovative ways.

Further, although the SSDF notes that "organizations should adopt a risk-based approach to determine what practices are relevant, appropriate, and effective to mitigate threats to their software development practices," it does not sufficiently address how a proven, effective, risk-based approach would interact with the EO's requirement of "attesting to conformity with secure software development practices." In short, resources used to check the boxes of the requirements cannot be used in a risk-based approach to achieve the goal of reducing the number of vulnerabilities in software, and the SSDF would be improved with additional consideration of how a risk-based and requirement-based approach interact.

BSA is also interested in how software developers would demonstrate conformance with the practices or tasks identified. Once NIST (and subsequently OMB pursuant to Section 4(k) of the EO) determines the requirements, how will the US Government determine if software conforms to its requirements, and who will attest that conformance has been demonstrated? If self-attestation is insufficient and a third-party is required, will NIST act as the third party and if not, what organization will? Further, particularly in light of how frequently software is updated

[2] The ten activities contained in Section 4(e) are: (i) secure software development environments; (ii) generating and, when requested by a purchaser, providing artifacts that demonstrate conformance to the processes set forth in subsection (e)(i) of this section; (iii) employing automated tools, or comparable processes, to maintain trusted source code supply chains, thereby ensuring the integrity of the code; (iv) employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at a minimum prior to product, version, or update release; (v) providing, when requested by a purchaser, artifacts of the execution of the tools and processes described in subsection (e)(iii) and (iv) of this section, and making publicly available summary information on completion of these actions, to include a summary description of the risks assessed and mitigated; (vi) maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis; (vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website; (viii) participating in a vulnerability disclosure program that includes a reporting and disclosure process; (ix) attesting to conformity with secure software development practices; (x) ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product.

to improve both security and functionality, how does the US Government expect to obtain assurance in the future? To what extent will determination, attestation, or surveillance be automated or manual? The answers to these questions will impact the effectiveness of the practices but also the administrative burden to software developers and the costs to agencies. Moreover, answers to these questions could increase the cost without a corresponding increase in the security of the software.

BSA supports the goals of the EO generally, and the work of improving the security of software under Section 4(e) specifically, but thinks it is important that NIST and OMB ensure software developers have sufficient time to "integrate the SSDF throughout their existing software development practices." Without sufficient time, developers will be unable to meet requirements and provide the secure software solutions needed to accomplish the US Government's mission. Further, the SSDF should make clear that secure software development does not require the divulgence of source code or other proprietary information.

Finally, in a shared recognition that "the security of software used by the Federal Government is vital to the Federal Government's ability to perform its critical functions," BSA recommends NIST (and subsequently OMB pursuant to Section 4(k)) clarify that any guidance or requirements for the development of software is also applicable to software developed by the Federal Government. Clearly, to achieve the goal of improving software security, the Federal Government should follow any guidance or requirements that the Federal Government would impose on companies that provide it software. If the Federal Government's commitment to comply with such guidance and requirements is not clarified, it will greatly undermine confidence in the US Government's commitment and ability to improve software security.

Thank you for the opportunity to provide these comments. BSA looks forward to continuing to work with NIST to further improve software security.

Sincerely,

Henry Young
Director, Policy