May 26, 2021

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

Via e-mail to swsupplychain-eo@list.nist.gov

Re: Position Paper on Standards and Guidelines to Enhance Software Supply Chain Security

Dear Mr. Stine,

BSA | The Software Alliance[1] appreciates the opportunity to provide this position paper to help identify standards, tools, best practices, and other guidelines to enhance software supply chain security. 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 enterprise 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 shares the President's view that "[t]he security of software used by the Federal Government is vital to the Federal Government's ability to perform its critical functions." Indeed, BSA believes this to be true for private sector organizations as well. BSA is pleased to see NIST directed to lead the centerpiece of the Executive Order: working with industry and academia to identify existing and develop new standards to continue to enhance software security.

NIST's forthcoming guidance should recognize that managing software security risk is a continuous process. Software developers use iterative approaches, and the software security community constantly develops better testing methodologies. Notably, NIST's own National Vulnerability Database has received more than 100 new critical vulnerabilities and exposures last week alone demonstrating that a scan of known vulnerabilities will quickly become obsolete. Single point-in-time testing is simply not a replacement for well-developed and sustained software security risk management practices.

To achieve its goals, NIST is seeking position statements in five areas.

1. Criteria for designating "critical software." BSA recognizes the challenge of defining "critical software." The definition ought to be (1) targeted, neither over nor under inclusive; (2) clear, needing no further interpretation or explanation; (3) predictable, enabling participants throughout the software supply chain to know its impact; and (4) stable, unchanging from design through disposal.

---

[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, and Workday.

2. An "[i]nitial list of secure software development lifecycle standards, best practices, and other guidelines acceptable for the development of software for purchase by the Federal Government." Like NIST, BSA has been working on strengthening software security policies for many years. More than two years ago, BSA launched its Framework for Secure Software—a risk-based, outcome-focused, flexible, and standards-based risk management tool for developers and suppliers, but also for vendors, customers, and policymakers.

The BSA Framework for Secure Software builds on industry best practices, internationally recognized security standards, and government guidance to provide a common organization and structure to software security's complex challenges and different technical approaches. Notably, BSA's Framework for Secure Software maps to NIST's Secure Software Development Framework (SSDF) and it can help any organization evaluate software security outcomes, communicate those security outcomes to a variety of stakeholders, and manage software security risk.

The BSA Framework for Secure Software drives more secure software and improved risk management practices by focusing on three areas: (1) secure development, (2) secure capabilities, and (3) secure lifecycle. In turn, each of these three areas contains categories, subcategories, diagnostic statements, implementation notes, and informative references that guide down potential paths to improve software security.

BSA recommends NIST identify the BSA Framework for Secure Software as a best practice, the use of which would make the underlying software acceptable for purchase by the Federal Government.

3. Guidelines outlining security measures that shall be applied to the Federal Government's use of critical software. The software security practices identified in the BSA Framework include numerous diagnostic statements related to least privilege, network segmentation, and proper configuration. Further, many of these diagnostic statements map to NIST's SSDF. BSA therefore recommends identifying the BSA Framework as a set of best practices for use with critical software in the initial period.

4. Initial minimum requirements for testing software source code. With the appreciation that testing is not substitute for a wholistic approach to secure development, capabilities, and lifecycle, the BSA Framework provides an entire category of testing and verification, including relevant standards and informative references.

5. Guidelines for software integrity chains and provenance. The BSA Framework provides diagnostic statements, relevant standards, and informative references for software integrity, including SAFECode's Software Supply Chain Integrity Framework.

# # # # #

BSA looks forward to participating in NIST's Enhancing Software Supply Chain Security Workshop. Thank you for the opportunity to comment on this important matter and for your continued work on software security.

Sincerely,

Henry Young
Director, Policy