August 5, 2019

Donna Dodson
Murugiah Souppaya
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Via email to: ssdf@nist.gov

Re: Comments on Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)

Dear Ms. Dodson and Mr. Souppaya:

BSA | The Software Alliance[1] appreciates the opportunity to provide comments on the National Institute of Standards and Technology's (NIST's) Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF) white paper draft (Draft). BSA is the leading advocate for the global software industry before governments and in the international marketplace. Software powers technologies that enhance our personal lives and businesses in every sector, and BSA's members are at the forefront of software-enabled innovation, including the Internet of Things, blockchain, and artificial intelligence. Moreover, BSA's members are pioneers in the field of software security, leading the development of principles relating to the secure software development lifecycle (SDLC) and security-by-design.

The software community has developed methods and tools to help software developers address important aspects of software security, including security-by-design principles, secure development lifecycle processes, and internationally recognized standards, and BSA members pioneered many of the software security best practices utilized across the industry today. BSA recognizes that effective security requires a comprehensive and risk-informed approach that combines individual security considerations into a holistic, lifecycle-long framework. Accordingly, BSA developed and launched earlier this year the *BSA Framework for Secure Software*, a first-of-its-kind tool for describing and assessing software security through a flexible, outcome-based, risk-informed methodology. The BSA Framework addresses both organizational processes and product security capabilities to inform and assess software security throughout its lifecycle.

BSA commends NIST for its leadership in developing foundational recommendations for a core set of high-level secure software development practices. Such guidance is urgently needed as the number and range of products that rely on software rapidly expands and the

[1] BSA's members include: Adobe, Akamai, Apple, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens PLM Software, Sitecore, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

security threat landscape continues to evolve. BSA also appreciates NIST's collaboration in the drafting of its White Paper, and its comprehensive integration of key concepts from BSA's *Framework for Secure Software*.

BSA commends NIST for developing a draft that is outcome-focused and adaptable. Rather than prescribe specific security techniques or technologies, the Draft outlines Tasks that identify actions organizations can take to achieve beneficial security outcomes. Importantly, these outcome-oriented Tasks are neutral with respect to coding language, development process, and technical approach. Similarly, BSA applauds the White Paper's adaptable approach to software security. Software is constantly changing in today's development environment. Furthermore, many products are continually updated with new features and additional security measures long after their original market deployment. Any approach to software security must be able to adapt to the constant innovation of new technologies, processes, and standards in the software industry.

While the adaptable, outcome-focused approach adopted by the White Paper is conducive to a risk-based approach, the White Paper does not explicitly articulate guidance on understanding risk and applying Tasks or Implementation Examples according to risk. The White Paper should be updated to clarify the role of risk and provide guidance, both to help developers understand how to implement a risk-informed application of the Framework and to help organizations communicate implementation decisions to software consumers.

Furthermore, BSA is concerned that the Tasks are, in some cases, insufficiently detailed to address core SDLC elements that are critical to guiding effective implementation of the Framework and improving software security. More specifically, the White Paper covers several important topics in the "Implementation Examples" column rather than including them as Tasks, thereby offering limited detail and suggesting that their inclusion in an SDLC is non-essential. BSA recommends that NIST consider reviewing the Implementation Examples with a view toward identifying those that should be replicated as core processes across all SDLCs and converting them to Tasks. In particular, BSA highlights the following Implementation Examples as priorities for reconsideration given their importance to secure software development:

Task Reference	Implementation Example	Rationale
PO.1.1	"Define policies that specify the security requirements for the organization's software to meet, including secure coding practices for developers to follow."	Every software developing organization should establish and document recognized, enforceable coding standards and canonical data formats.
PO.1.1	"Ensure policies cover the entire software life cycle, including notifying users of the impending end of software support and the date of software end-of-life, when the software will no longer function properly."	Consistent, transparent, predictable end-of-life guidelines are critical to ensure that users are able to avoid using unsupported and potentially insecure software or to take measures mitigating risks associated with such software. End-of-life considerations should be incorporated into the SDLC, facilitating consideration of the anticipated duration and terms of support, the processes for communicating end-of-life guidance and

		changes to that guidance to consumers, and similar issues as the software is developed and as a key element of software maintenance.
PS.1.1	"Use version control features of the repository to track all changes made to code with accountability to the individual developer account."	Change management is important for both quality control and security. Using version control features within a repository is one, but not the only, approach to change management. Regardless of the approach, organizations should maintain an up-to-date product history documenting all changes to software elements and configurations. Ideally, this documentation should track the origin of code (date, time, rationale, responsible individual) on a line-by-line basis.
PW.1.1	"Perform more rigorous assessments for high-risk areas, such as protecting sensitive data."	NIST should consider whether the Framework should dedicate a Task to more specifically consider how sensitive data should be identified or defined and protected, given how important such consideration is to developing strategies for the use of encryption and other security controls and features.
PW.3.2	"See if there are publicly known vulnerabilities in the software modules and services that the vendor has not yet fixed."	Reviewing and testing third-party components for vulnerabilities is a critical part of software supply chain risk management, and should be incorporated into any SDLC.
PW.5.1	"Validate all untrusted input, and validate and properly encode all output;" "avoid using unsafe functions and calls;" "handle errors gracefully;" and "provide logging and tracing capabilities."	These examples each represent core guidelines of secure coding and should be performed as Tasks in every SDLC.

Software security is one of the most pressing challenges we face in the cybersecurity arena, and BSA and its members are eager to work with NIST to encourage more robust security measures across the software industry. We hope our recommendations will support NIST's efforts to promote best practices for software security. Thank you for the opportunity to comment on this important matter.

Sincerely,

Tommy Ross
Senior Director, Policy

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org