BUSINESS SOFTWARE ALLIANCE RESPONSE TO THE INITIAL PUBLIC DRAFT OF THE SECURE SOFTWARE DEVELOPMENT FRAMEWORK VERSION 1.2

The Business Software Alliance (BSA) appreciates the opportunity to comment on the Initial Public Draft of the Secure Software Development Framework (SSDF) 1.2. BSA strongly supports the SSDF's objective to help "software producers reduce the number of vulnerabilities in released software, mitigate the potential impacts of the exploitation of undetected or unaddressed vulnerabilities, and address the root causes of vulnerabilities to prevent future recurrences." These goals closely align with the principles reflected in the BSA Framework for Secure Software, which the SSDF cites nearly 40 times, underscoring the strong alignment between NIST's approach and other industry best practices.

BSA (www.bsa.org) is the global trade association of the enterprise software industry, representing companies[1] that are leaders in cybersecurity, artificial intelligence, cloud computing, and other cutting-edge technologies. We advocate policies that build trust in technology so that every industry sector and the public can benefit from innovation.

BSA appreciates NIST's clear emphasis on the need for a risk-based approach to secure software, including the recognition that not all practices will be applicable to every use case. The draft appropriately acknowledges that organizations must assess which practices are relevant, appropriate, and effective based on their specific threat environments and operational contexts. We also welcome NIST's broad and accurate characterization of vulnerabilities as encompassing not only coding flaws, but also weaknesses arising from misconfigurations, incorrect trust assumptions, and outdated or incomplete risk analysis. This framing reflects the realities of modern software development and use, and reinforces the importance of addressing security holistically across people, processes, and technology.

To further strengthen the SSDF, with the goal of ensuring the framework remains risk-based, practical to implement, and consistent with secure software development practices already widely adopted across the software ecosystem, BSA recommends NIST revisit PS.3.2.

[1] BSA's members include: Adobe, Alteryx, Amadeus, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cohere, Cohesity, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

200 Massachusetts Avenue, NW Suite 310 Washington, DC 20001
202.872.5500 **www.bsa.org**

Under PS.3 "Archive and Protect Each Software Release (PS.3): Preserve software releases in order to help identify, analyze, and eliminate vulnerabilities discovered in the software after release," task PS.3.2 suggests that an organization "Collect, safeguard, maintain, and share provenance data for all components of each software release (e.g., in a software bill of materials [SBOM])."

BSA is concerned that the use of the term "share" could be misinterpreted to suggest an expectation that software producers publish provenance data or otherwise provide it broadly without appropriate controls. This concern is reinforced by the fact that Examples 1 and 2 under PS.3.2 instead use the phrase "make the provenance data available," which implies a different and more limited meaning than "share."

Such a misinterpretation could undermine a software producer's ability to safeguard provenance data, despite safeguarding provenance data being an explicit element of the task itself. By contrast, the language used in Examples 1 and 2 more accurately reflects the need for controlled, risk-based access to provenance data rather than unrestricted dissemination.

Accordingly, BSA recommends that NIST revise Task PS.3.2 to align with the language used in Examples 1 and 2, and read: "Collect, safeguard, maintain, and make available provenance data for all components of each software release . . ." This change would improve clarity and help ensure the task is applied in a risk-based manner consistent with established secure software development practices.

* * *

BSA appreciates NIST's continued leadership in advancing secure software development practices, as well as the recognition of the value of the BSA Framework for Secure Software, and the opportunity to comment on the draft SSDF Version 1.2. We look forward to continued engagement with NIST as the framework is refined.

Sincerely,

Henry Young
Senior Director, Policy