December 10, 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 scrm-nist@nist.gov

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) Special Publication (SP) 800-161, Revision 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.

BSA is the leading advocate for the global enterprise software industry before governments and in the international marketplace. BSA 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 security, having pioneered many of the software security best practices used throughout the industry today, including The BSA Framework for Secure Software.

The BSA Framework for Secure Software, which NIST's own Secure Software Development Framework (SSDF) references and maps to, also highlights software supply chain risk management. For example, the BSA Framework for Secure Software identifies software supply chains as a key category of secure software development and includes 6 additional subcategories and 12 corresponding diagnostic statements regarding software supply chain security.

[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.

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

P 202-872-5500
W bsa.org

BSA understands that, while SP 800-161 was originally published in April 2015, and updated prior to President Biden signing the Executive Order (EO) on Improving the Nation's Cybersecurity, NIST is now updating the document to respond to that EO.

BSA shares and supports the goals of the EO on Improving the Nation's Cybersecurity, including improving the cybersecurity risk management of the software supply chain. As a preliminary matter, BSA notes that the US Government is currently undertaking numerous supply chain security activities, including implementing the EO on Securing the Information and Communications Technology and Services Supply Chain signed by President Trump in May 2019, the EO on America's Supply Chains signed by President Biden in February 2021, the EO on Improving the Nation's Cybersecurity, signed by President Biden in May 2021, and the EO on Protecting Americans' Sensitive Data from Foreign Adversaries signed by President Biden in June 2021. In general, it would be helpful for the US Government to clarify if and how these and other efforts are related.

With regards to NIST SP 800-161 specifically, first, NIST should consider shortening and structing this guidance to align with the NIST SSDF and the NIST Cybersecurity Framework. Organizing this document similarly to the NIST SSDF and Cybersecurity Framework would make the document more usable and, in turn, improve communications between software developers and their US Government customers.

Additionally, it would be helpful to locate all content related to secure software development in the NIST SSDF. As guidance on cybersecurity, software security, and supply chain security risk management continues to increase in breadth and depth, to ensure public and private sector organizations can locate and understand guidance, it is increasingly important to have an authoritative source for information on a topic. To the extent SP 800-161 can and should include information about secure software development, it should do so through references to the NIST SSDF as well as best practices and international standards.

Similarly, any consideration of software bills of materials (SBOMs) should be contained in the SSDF and incorporated into SP 800-161 by reference. Further, NIST should explicitly recognize the limitations of SBOMs as an emerging technique to manage supply chain and cybersecurity risk. An SBOM can provide useful information to a customer but, without additional context, can also be misleading and result in suboptimal action. For instance, an SBOM may identify a vulnerable component that cannot be exploited as used but may nonetheless lead an organization to compel a software developer to addresses that unexploitable vulnerability. Alternatively, even if an SBOM identifies a vulnerability that is exploitable, an SBOM may inappropriately prioritize the use of cybersecurity resources as there may be more effective ways to address the vulnerability or otherwise improve the security of the product or service.

"Federal agency personnel," NIST's intended audience for SP 800-161, likely understand an SBOM's limitations, and that an SBOM is a piece of a broader cybersecurity risk management puzzle. However, other organizations, including those outside the US, look to NIST as a leading authority for cybersecurity risk management and without further clarification, these organizations may improperly

rely on an SBOM. Because SBOMs are an emerging tool, NIST should be explicit that they are intended to provide supplemental information and do not themselves provide sufficient information on which an organization can measure either the risk or quality of the software they describe, nor do they identify the most effective use of cybersecurity resources.

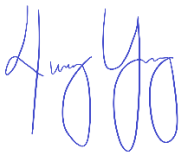
NIST should also clarify the risk associated with the publication of an SBOM, whether intentional or unintentional. For example, if an SBOM is used as a tool for vulnerability disclosure practices, there is the risk that it will provide a roadmap for bad actors to exploit software. For this and other reasons, customers, including US Government customers, should apply appropriate security controls to an SBOM, just as they would other supply chain information.

Second, NIST should consider how it can streamline compliance and conformance and avoid duplication for any voluntary or mandatory activities. Appendix F suggests preferencing or mandating that software developers provide a new "software security label or data sheet" which potentially creates a duplicative compliance activity for risks that already are addressed through the implementation of the NIST SSDF and development of a proposed SBOM. BSA encourages NIST to leverage and reference existing standards, best practices, and certifications to demonstrate conformance.

Third, while NIST's work on consumer cybersecurity labeling may prove useful, it remains in a pre-pilot phase and is aimed at consumers, not departments and agencies or their industry partners. Again, to the extent SP 800-161 needs to identify issues associated with the labeling of consumer products, it should do so only through references to external documents, including those that NIST may publish in response to the EO on Improving the Nation's Cybersecurity, Section 4(s).

Finally, NIST should strongly consider publishing a standalone EO Section 4 Road Map to detail all practices an organization must adopt to meet requirements under Section 4. Such a document could consolidate the mappings from SP 800-161, Appendix F and the SSDF, Appendix A, as well as any other requirements. BSA notes that SP 800-161, Appendix F focuses on EO-Critical Software but that NIST's Critical Software Definition - Introduction notes that "The requirements 4e and 4k related to acquisition apply to all software, not just critical software." A standalone Section 4 Road Map could clarify which practices apply to EO Critical Software and which to all software.

BSA looks forward to continuing to work with NIST to improve software security generally and software supply chain security specifically.



Henry Young
Director, Policy

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

P 202-872-5500
W bsa.org