June 17, 2021

Evelyn L. Remaley
Acting Administrator
National Telecommunications and Information Administration
1401 Constitution Avenue NW
Room 4725
Washington, DC 20230

Via email to SBOM_RFC@ntia.gov

Dear Acting Administrator Remaley:

BSA | The Software Alliance[1] appreciates the opportunity to comment on the National Telecommunications and Information Administration's (NTIA) Request for Comment on Software Bill of Materials Elements and Considerations (Docket No. 210527-0117, RIN 0660-XC051).

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.

The recently released Executive Order (EO) on Improving the Nation's Cybersecurity seeks to enhance the security of the Federal Government's information technology and operational technology systems, including through government-procured products and services. BSA supports the aims of the EO and has long advocated the importance of prioritizing security throughout governments' acquisition processes.

Section 4(f) of the EO directs the Secretary of Commerce, in coordination with the Assistant Secretary for Communications and Information and the Administrator of NTIA, to publish minimum elements of a software bill of materials (SBOM). As the Department of Commerce fulfills this requirement of the EO, for NTIA's consideration, BSA shares the following recommendations on SBOM generally and on the specific minimum elements of an SBOM outlined in NTIA's request.

[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, Workday, and Zoom.

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

P 202-872-5500
W bsa.org

I. General Comments on SBOM

A. Ensuring Optimal Use of Cybersecurity Resources

BSA supports the EO because, in general, it appropriately prioritizes activities that have high benefit-cost ratios, for example, migrating to the cloud, implementing multifactor authentication, and encrypting data "to the maximum extent consistent with . . . applicable laws." In addition, improving software development practices will improve the entire cybersecurity ecosystem. An SBOM, if properly tailored and aligned with international standards, can provide useful information to customers, but if too prescriptive or not understood as a smaller part of a larger cybersecurity risk management program, can offer misleading information or simply not be a useful security investment.

Put simply, US agencies (like all organizations) are resource-constrained and therefore, must make tradeoffs. Detecting vulnerabilities through an SBOM requires mapping component identity fields to existing vulnerability databases. This mapping will not, however, explain if the component is used in a manner that would allow the vulnerability to be exploited. An SBOM is likely to cause a US agency to reprioritize its actions, in response to a vulnerability identified through an SBOM even if the software is *not exploitable as used*. If required to expend resources to remediate the identified non-exploitable vulnerability, then that agency cannot use those resources on cybersecurity activities that it would otherwise, correctly, identify as higher priority. For example, research indicates that for Java, Ruby, and Python, "less than 5% of products that contain a library with a vulnerability are vulnerable."[2] In short, use of an SBOM not properly incorporated into a broader cybersecurity risk management program, will lead to suboptimal use of resources, and reduce the impact of the EO.

BSA recommends NTIA explicitly recognize that while an SBOM can improve cybersecurity it is appropriately understood as a smaller piece of a larger cybersecurity risk management program and that a vulnerability identified by an SBOM might not actually be exploitable.

B. Applying SBOM to SaaS

The Executive Order helpfully directs the acceleration of the "movement to secure cloud services, including Software as a Service (SaaS)." While this movement will help agencies reduce their cybersecurity risk, SaaS is a particularly challenging use case for an SBOM. Vendors update software in many cloud environments and SaaS offerings daily, if not more frequently, making an SBOM instantly obsolete.

[2] "How Understanding Risk Is Changing for Open Source Components"
Presentation at the RSA Conference 2019 by Chris Wysopal, CTO & Co-founder Veracode, Session ID: PDAC-R11, available at:
https://www.ntia.doc.gov/files/ntia/publications/wysopal_swct_kickoff_perspective.pdf

An SBOM is often compared to a "food label" to explain its utility. However, in the context of SaaS, the analogy crumbles. The contents of a box of cookies does not change between the time the company develops the recipe, manufacturers the cookies, packages them in a box, or ships them to a store. The contents do not change between the time the cookies are purchased, stored, or eaten. Similarly, the health and safety of the cookies do not change based on the context one eats them. In contrast, SaaS will almost certainly be updated numerous times between any of the above steps and continue to be updated during its use. Finally, unlike a box of cookies, the context in which SaaS is used affects its risk.

BSA recommends that NTIA explicitly recognize that, presently, an SBOM is not an effective tool for SaaS, and that moving forward there needs to be flexibility to accommodate different use cases.

II. Minimum Elements of an SBOM

Turning to the minimum elements that NTIA has proposed, to achieve the goals of the EO and improve the entire cybersecurity ecosystem, an SBOM needs to be based on a voluntary consensus standard, not on a government specific standard. International standards provide widely vetted, consensus-based information and guidance for defining and implementing effective security methodologies, and facilitate common approaches to common challenges, thus enabling collaboration and interoperability.

As noted in the Survey of Existing SBOM Formats, some of these standards have existed and been used for nearly a decade and experts have already mapped these standards to the minimum elements NTIA proposes in its RFC. That is, as directed by the National Technology Transfer Advancement Act[3] and OMB Circular A-119,[4] the Federal Government can use existing voluntary consensus standards to achieve its policy objectives. BSA recommends NTIA rely on existing voluntary consensus standards to advance this work.

As described in BSA's Framework for Secure Software, software developers should, to the extent feasible, develop software in a way that is informed by supply chain risk management practices, and ensure the visibility and traceability, and security of third-party components. Practices like these provide customers, including the Federal Government, confidence that they know what they are purchasing.

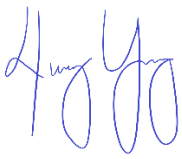
[3] The National Technology Transfer and Advancement Act of 1995 (NTTAA), Pub. L. 104-113, Sec. 12(d)(1), "all Federal agencies and departments shall use technical standards that are developed or adopted by voluntary consensus standards bodies, using such technical standards as a means to carry out policy objectives," available at: https://www.govinfo.gov/content/pkg/PLAW-104publ113/pdf/PLAW-104publ113.pdf.

[4] 81 FR 4674, Revision of OMB Circular A-119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities" (Jan. 1, 2016), "directs agencies to use standards developed or adopted voluntarily consensus standards bodies rather than government-unique standards, except where inconsistent with applicable law or otherwise impractical," available at: https://obamawhitehouse.archives.gov/omb/circulars_a119_a119fr#:~:text=The%20policies%20of%20OMB%20Circular,reliance%20on%20government%2Dunique%20standards.

Operational considerations related to delivering an SBOM are also important. Requiring a company to publish an SBOM, especially when software is not managed by the customer, would not improve a customer's cybersecurity risk management, and may unintentionally assist adversaries. Further, targeting how deep an SBOM goes will improve an SBOM's efficacy, that is, by requiring too much information on too many levels of relationships, an SBOM will actually become less useful.

Thank you for the opportunity to comment on this important matter and for your consideration of our views. BSA looks forward to working with NTIA to effectively implement the EO.

Sincerely,



Henry Young
Director, Policy

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

P 202-872-5500
W bsa.org