Comments from BSA | The Software Alliance on the Draft Guidance on Introduction of Software Bill of Materials (SBOM) for Software Management Ver. 2.0

May 27, 2024

General Comments

BSA | The Software Alliance (**BSA**)[1] appreciates the opportunity to provide the comments below in response to the public consultation on the "Draft Guidance on Introduction of Software Bill of Materials (**SBOM**) for Software Management Ver. 2.0" (**Draft Guidance**) by Ministry of Economy, Trade, and Industry (**METI**).[2]

BSA is the leading advocate for the global software industry. BSA members are among the world's most innovative companies that help to drive digital transformation by providing the solutions that make businesses and governments more competitive and effective. BSA members provide various tools including identity and access management, data analytics, cloud storage and data processing services, customer relationship management software, human resource management programs, and collaboration systems.

BSA shares METI's concern about software security — "enhancing software security" is our first priority in BSA's 2024 Global Cyber Agenda.[3] Improving software security will require a multifaceted approach. BSA's agenda considers SBOMs specifically, and we recommend industry and governments to continue working together to standardize SBOMs. SBOMs are not a panacea but can expedite incident response once customers are prepared to use them. In this sense, we welcome METI taking a voluntary approach and conducting tests (Proof-of-Concepts) to evaluate the challenges and benefits of SBOM introduction in several industrial sectors.

Recognize the Software Bill of Materials (SBOM) as a Promising but Limited Tool

Modern software, and in particular cloud-based software delivered as a service, is much more likely to use a dynamic list of components. These components can number in the thousands. The dynamism and number of components complicate both the development and use of an SBOM and necessitate careful consideration to ensure that SBOMs improve cybersecurity. As the Draft Guidance illustrates, while SBOMs can be used for efficient software management,

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Cohere, Dassault, Databricks, DocuSign, Dropbox, Elastic, ESTECO SpA, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Nikon, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

[2] https://public-comment.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=595224009&Mode=0

[3] https://www.bsa.org/files/policy-filings/2024cyberagendabsa.pdf

22F Shibuya Mark City
1-12-1 Dogenzaka, Shibuyaku,
Tokyo 150-0043

P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org

Japan Representative Office

there are various issues that need to be addressed when actually implementing SBOMs. SBOMs, combined with the tooling, standards, and automation currently being developed, will improve cybersecurity. But they are not a comprehensive solution. SBOMs have not yet achieved the required maturity to be widely relied upon and there are no commonly used standards at this stage. For example, there is no single globally prescribed method for determining components names so two different SBOMs authors might use two different identifiers for the same component. This is because software components suppliers define component names according to their own needs. Moreover, while versions of certain SBOM formats can indeed be used to document vulnerabilities in addition to components contained in the product, this is certainly not its intended use. Vulnerabilities are sometimes discovered after product release, and vulnerability properties can change. Republishing entire SBOMs whenever vulnerabilities are discovered or modified therefore would be inefficient.

The cybersecurity community is working to create SBOMs that are verifiably accurate. As indicated in "2.5. Myths and facts," the fact that a software component listed in an SBOM is known to have an associated vulnerability does not indicate that the software represented by that SBOM is necessarily vulnerable. For example, as mentioned in footnote 17 of Draft Guidance, pairing an SBOM and product metadata with Vulnerability Exploitability eXchange (VEX) metadata is one way some practitioners are enabling machine-readable and automated analysis of software vulnerabilities, allowing an understanding to be established of whether a vulnerable component results in a vulnerable product. Such efforts are crucial to making SBOM consumable and valuable.

Challenges Specific to the Cloud Environment

Under "2.5. Myth and Facts", the draft Guidelines state that "SBOMs for online applications such as SBOMs for container images, SBOMs for SaaS software, and SBOMs for cloud services are also being discussed mainly in the U.S." In this regard, we want to highlight the challenges specific to the cloud environment: for example, updates and patches in Software-as-a-Service (SaaS) are usually done on a continuous basis (and automated). This leads to a faster resolution of vulnerabilities. Therefore, adopting SBOMs in the cloud context would be ineffective because the SBOMs would be outdated very quickly. As such, adopting, on a voluntary basis, SBOMs for on-premises software may be less challenging.

Limiting the Level of Detail to be Included in SBOMs to Expedite Their Delivery and Use

BSA supports the development and use of SBOMs but recommends, at least initially, limiting the scope of information to be included in SBOMs to focus on building their foundations. By limiting the level of detail and scope of information included in SBOMs, enterprises can begin to reap the benefits of SBOMs more quickly. This approach would not foreclose the possibility of building out additional requirements as industry develops the people, processes, and technologies needed to implement more detailed and comprehensive SBOMs.

Recommend SBOMs Only for Products with Digital Elements Used in Specific Contexts

Any recommendation to use SBOMs should apply only for products with digital elements used in specific contexts. As a first step, SBOMs might be used in specific cases. Section "2.5. Myth and Facts" states that "SBOM does not need to be made public. The act of making an SBOM is separate from sharing it with those who can use this data constructively" and also states that "SBOMs are a summary of included software components and do not expose intellectual property (IP) Patents and algorithms are not included." Consistent with this, it is important to

stress that public disclosure of SBOMs could pose a risk to intellectual property as well as to product security. As acknowledged in this section, while SBOMs alone do not provide highly sensitive trade secrets like source code, they can include other proprietary information such as the particular blend of software providers, vendors, and partners used to produce a given offering, which constitutes valuable intellectual property and proprietary information. Companies may provide an SBOM to their customers but should not be required to make that information public or otherwise disclose that information without proper safeguards, such as non-disclosure agreements. Additionally, using SBOMs for vulnerability disclosures or fully including them in the technical documentation could create a roadmap for malicious actors to exploit vulnerabilities.

Lastly, we want to highlight that there is important industry-government work happening to find and fill the gaps necessary to take SBOMs from the theoretical to concrete security improvements and governments should continue to be circumspect in implementing SBOMs before that work is complete.

Conclusion

BSA and our members look forward to working with METI to support the goal of controlling software vulnerabilities to enhancing software security. SBOMs are an important part of this work. To enable global software vendors, including BSA members, to contribute to the discussion and make detailed recommendations, we recommend preparing an English version of the draft document upon the time of public consultation. We would appreciate an opportunity to discuss how we can further assist in the effort.

22F Shibuya Mark City
1-12-1 Dogenzaka, Shibuyaku,
Tokyo 150-0043

P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org

Japan Representative Office