November 10, 2022

Thomas Cummings
Senior Software Engineer
Office of the Deputy Assistant Secretary of the Army for Data, Engineering, and Software
6007 Combat Drive F3-112
Aberdeen Proving Ground, MD 21005

Via e-mail to: thomas.a.cummings16.civ@army.mil; hadir.m.elba-parsons.civ@army.mil

Mr. Cummings:

BSA | The Software Alliance[1] appreciates the opportunity to provide the below comments in response to the Department of the Army's Request for Information (Notice ID W15QKN-23-X-0RR0).

BSA is the leading advocate for the enterprise technology sector. Our members are among the world's most innovative companies and help to drive digital transformation by providing the solutions that make businesses and governments more competitive and effective. These solutions include cloud computing, customer relationship management, human resources management, identity and access management, data analytics, manufacturing, and infrastructure tools and services.

BSA shares your concern about software security. Indeed, "Improving Software Security" is our first priority in Enhancing Cyber Policy, Advancing Digital Transformation: BSA'S 2023 Global Cyber Agenda. Improving software security will require a multifaceted approach, including leveraging the priorities highlighted in the Executive Order on Improving the Nation's Cybersecurity.

[1] BSA's members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Prokon, PTC, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

BSA's agenda considers SBOMs specifically, and we support "developing and using software bills of materials (SBOMs) as well as the associated tooling, standards, and automation necessary for transforming the information contained in an SBOM into concrete cybersecurity improvement."

BSA describes the state and promise of SBOMs in our August 31, 2022 blog, SBOMs: Considerable Progress, But Not Yet Ready for Codification. Multiple US Government agencies, including the National Telecommunications and Information Administration and the Department of Homeland Security, have identified gaps in SBOMs. BSA and its members are currently working with US Government partners and other stakeholders to address these and other gaps.

Additionally, 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 further consideration to ensure that SBOMs improve cybersecurity.

Against this backdrop, as well as OMB Memo 22-18, the Department of the Army is seeking information about the "acquisition, validation, ingest, and use of Software Bills of Material (SBOMs)." Specifically, the RFI asks "What barriers or challenges do you see in the future, due to these new SBOM requirements? Are there downstream effects you believe will have unintended consequences? Are there steps that can be taken today, to mitigate concerns in the future?" One foreseeable challenge is the balkanization of SBOM requirements made by each US Government agency, and the corresponding deleterious impacts on cybersecurity.

In our 2023 Cyber Agenda, we highlighted harmonizing policies within and between governments as a priority. Harmonization improves cybersecurity of both organizations and the digital ecosystem in numerous ways, including making it easier for customers to communicate what they need to meet their risk management goals and vendors to demonstrate how their solutions meet those needs.

Harmonized SBOM requirements will ensure that US Government customers and their vendors share a common understanding of an SBOM's security benefits and limitations. Harmonized SBOM requirements will also ensure that US Government customers get what they need, when they need it, and in a format that enables them to translate that information into action.

The goal of a harmonized, whole-of-government approach is not new. For example, in its 2011 Memorandum for Chief Information Officers, OMB set forth its vision of such an approach for cloud services. While the Federal Risk and Authorization Management

Program (FedRAMP) continues to work toward its promise, the Department of the Army and the US Government have an opportunity to make a harmonized, government-wide, cost-effective, risk-based approach to the development and use of SBOMs a reality.

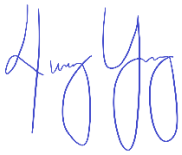
To help ensure that SBOMs deliver on their promise, the Department of the Army should:

- Partner with vendors to ensure that policies have net benefits both to the Department of the Army and to the broader digital ecosystem;
- Collaborate both with agencies inside the Department of Defense and those in the civilian government to harmonize requirements; and
- Build SBOM requirements on best practices and internationally recognized standards to support a secure and resilient marketplace for software solutions.

The Department of the Army specifically, and the US Government generally, should also work to harmonize requirements with those of like-minded countries.

Finally, though not considered specifically in the RFI, the Department of the Army should require its internal software developers, and its contactors, to meet all the requirements it imposes on its vendors, including the development and delivery of an SBOM. An organization's networks are only as strong as their weakest link. If the Department of the Army takes steps to secure only the portion of its software supply chain obtained through vendors, and not the portion developed by it or its contractors, the US Army will not have ensured "the software underpinning every aspect of its mission is secure and resilient to adversarial interference" as the RFI envisions.

BSA looks forward to working with the Department of the Army to improve the security of software, including the development and use of SBOMs.



Henry Young
Director, Policy

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org