November 22, 2022

The Honorable Jack Reed
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510

The Honorable James Inhofe
Ranking Member
Committee on Armed Services
United States Senate
Washington, DC 20510

Dear Chairman Reed and Ranking Member Inhofe:

We, the undersigned associations, have concerns with section 1627 of S. 4543, the "National Defense Authorization Act for Fiscal Year 2023." Section 1627 would require the Department of Defense (DoD) to establish requirements for a software bill of materials (SBOMs). SBOMs are expected to help organizations reduce cyber risk, but they will need processes, tools, and standards to translate SBOMs into improved cybersecurity outcomes. Governments, industry, and other stakeholders are already working to develop these processes, tools, and standards—efforts that are progressing at an impressive pace. The most constructive step Congress can take to help SBOMs deliver their anticipated benefits is to support this ongoing work and ensure that future laws requiring SBOMs are harmonized across the U.S. government.

We urge you to hold this legislation until a later date, while allowing the many executive branch activities related to SBOMs to mature the ecosystem. There are four points that support delaying the implementation of legislation on SBOMs.

First, the July 2021 Cyber Safety Review Board (CSRB) report on the Log4j event highlights the need for greater maturity around the development of SBOMs before they are written into law. "As designed today," the CSRB says, "SBOMs are limited, for example by variances in field descriptions and a lack of version information about catalogued components, and lack of automation on the consumption end due to these variances."[1]

Second, Congress and the administration are taking an uncoordinated approach to policymaking on SBOMs at a time when there is a growing consensus in favor of harmonizing federal cybersecurity requirements. The Senate would set requirements for DoD, and the House would set requirements for the Department of Homeland Security. Modern software is highly interconnected, so taking disparate approaches to SBOM policymaking would further complicate an already complex, emerging environment. This is especially important regarding evolving standards and best practices for managing the risk-based communication of SBOMs and the handling of and disclosure of software vulnerabilities.[2]

[1] https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf

[2] To reduce the risk of exploitation by malicious actors, information concerning vulnerabilities is kept in strict confidence during the coordinated vulnerability disclosure and handling (CVD) process until mitigations are publicly available. These practices are embodied in binding operational directives issued by CISA and international standards for CVD, as well as endorsed by Congress. See the IoT Cybersecurity Improvement Act of 2020 (P.L. 116-207) and the Cyber Incident Reporting for Critical Infrastructure Act (P.L. 117-103).

Third, SBOM legislation enacted now would get ahead of federal policies, particularly Executive Order 14028, *Improving the Nation's Cybersecurity* (May 2021), which calls for establishing baseline security standards for development of software sold to the government, including requiring developers to maintain greater visibility into their software and making security data publicly available. The Office of Management and Budget (OMB) announced on September 14, 2022, that agencies "must only use software" provided by software providers who can attest to complying with the government-specified secure software development practices developed by the National Institute of Standards and Technology.[3]

Under the EO, the OMB is allowing agencies to request SBOMs based on the comparatively undefined guidance in the National Telecommunications and Information Administration's July 2011 report, *The Minimum Elements for a Software Bill of Materials*.[4] The report highlights that there is a clear need for "convergence and uniformity" on SBOMs policymaking and implementation. The report further notes, "organization would incur non-trivial costs to handle a wide range of SBOMs implementations that are not easily compatible."

OMB's approach reflects a comprehensive government-wide approach that is preferable to congressional mandates directed at one agency that risk prematurely locking in technical and operational approaches for the foreseeable future. Left unchecked, these varying mandates can be expected to conflict in design and execution. Our associations believe that DoD should study the usefulness and suitability of acquiring an SBOM for noncommercial, commercial, and open-source software.

Fourth, an SBOM is often likened to a list of ingredients on a food package—but such analogies are misleading. The ingredients of packaged food do not change after they are produced, whereas most software continues to evolve and change throughout its lifecycle. Given the changing nature of software and the cybersecurity ecosystem in which it operates, overly simplistic analogies do a disservice to the broad and complex nature of formats, procedures, uniformity, and protections that are needed to make SBOMs manageable at scale.

Any requirements related to patching should be developed in a manner consistent with industry best practices and international standards (e.g., ISO/IEC 30111, 29147) for coordinated vulnerability handling and disclosure.[5]

---

[3] The two foundational NIST guidance documents are the Secure Software Development Framework, SP 800-218; the Software Supply Chain Security Guidance.
https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf

[4] https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

[5] CISA, "New Federal Government Cybersecurity Incident and Vulnerability Response Playbooks," November 16, 2021.
https://www.cisa.gov/uscert/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability

IoT Cybersecurity Improvement Act of 2020 (P.L. 116-207).
https://www.congress.gov/bill/116th-congress/house-bill/1668.

***

Policymakers in the executive branch and Congress should recognize that while SBOMs are advancing well in some areas of technology—which our associations are pleased to see—they need more time to mature from a more macro standpoint to reach ample standardization and scalability. Uncoordinated policies and legislation could easily disrupt this progress. Our associations are committed to partnering with you to ensure that SBOMs work for both the businesses community and agencies rather than see them unintentionally become an unproductive procurement and/or regulatory instrument.

Sincerely,

The Alliance for Digital Innovation (ADI)
BSA | The Software Alliance
Center for Procurement Advocacy (CPA)
The Cybersecurity Coalition
U.S. Chamber of Commerce

cc: Members of the Senate Committee on Armed Services
cc: Members of the Senate Committee on Homeland Security and Governmental Affairs
cc: Members of the House Committee on Armed Services
cc: Members of the House Committee on Homeland Security
cc: Cybersecurity and Infrastructure Security Agency
cc: Office of the National Cyber Director