September 14, 2022

The Honorable James Reed, Chairman, Senate Armed Services Committee

The Honorable James Inhofe, Ranking Member, Senate Armed Services Committee

The Honorable Gary C. Peters, Chairman, Senate Homeland Security & Governmental Affairs Committee

The Honorable Rob Portman, Ranking Member, Senate Homeland Security & Governmental Affairs Committee

The Honorable Adam Smith, Chairman, House Armed Services Committee

The Honorable Mike Rogers, Ranking Member, House Armed Services Committee

The Honorable Bennie G. Thompson, Chairman, House Committee on Homeland Security

The Honorable John Katko, Ranking Member, House Committee on Homeland Security

Dear Chairmen Reed, Peters, Smith, and Thompson, and Ranking Members Inhofe, Portman, Rogers, and Katko,:

We are writing to express our concerns about requirements in the recently passed U.S. House of Representatives National Defense Authorization Act (NDAA) Section 6722, "DHS Software Supply Chain Risk Management."[1] The requirements in this section jump ahead of in-progress administration and industry efforts by requiring holders of existing covered contracts and those responding to requests for proposal (RFP) from the U.S. Department of Homeland Security (DHS) to provide a bill of materials (BOM), certify the items in the BOM are free of vulnerabilities or defects, and identify a plan to mitigate any identified vulnerabilities.

The Information Technology (IT) industry agrees with Executive Order 14028 that improving software supply chain security is critical to ensuring the security of federal IT systems.[2] We support a risk management approach to mitigating vulnerabilities. Software bill of materials (SBOMs) offer a potential means to help organizations improve their risk management capabilities. However, the language in the NDAA is not sufficiently scoped nor does it account for current administration efforts regarding SBOMs, or the readiness of software suppliers and consumers, including government customers, to fully leverage SBOMs.

[1] https://www.congress.gov/bill/117th-congress/house-bill/7900/text

[2] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

The Amendment is Vague and Internally Inconsistent

The amendment would require a vendor to provide BOM as part of its response to a DHS RFP to be used as part of the proposal evaluation process. As drafted, the amendment is unclear on whether the bill of materials is limited to software or all components. An expansion beyond software is inconsistent with existing administration efforts, impractical and introduces additional implementation challenges. Furthermore, paragraph (e) of the amendment provides conflicting requirements with respect to certifications and notifications. In one instance, the provision requires certification that the items in the BOM are free of vulnerabilities or defects, and in another it requests a plan to mitigate all identified vulnerabilities. These provisions would be problematic because they could prevent DHS from acquiring nearly any of the latest most capable and most secure technologies, significantly limiting DHS' ability to contract with traditional and nontraditional contractors that do not have a BOM. In turn, this would limit DHS' vendor base.

The Amendment is Premature and Conflicts with Existing Administration Efforts

We are also concerned that a requirement to mitigate all identified vulnerabilities is moving both industry and government away from the risk management guidelines[3] from the National Institute of Standards and Technology (NIST). It is also at odds with the recommended practices contained in the just released Securing the Software Supply Chain guide published by the Office of the Director of National Intelligence, the National Security Agency and CISA[4]. Not all vulnerabilities are the same and they should not all be treated the same way. Organizations should be able to prioritize which vulnerabilities to mitigate, based on their own risk assessments in the products and in their own environments, which is consistent with the requirements adopted under DHS Cybersecurity and Infrastructure Security Agency (CISA) Binding Operational Directive (BOD) 22-01[5]. There are low risk and non-exploitable[6] vulnerabilities for which there are, appropriately, no plans to address.

Additionally, federal guidance around SBOM is still being developed, with the National Telecommunications and Information Administration (NTIA) and CISA just completing listening sessions and standing up working groups.[7] The White House Office of Management and Budget is working on guidance[8] to agencies about SBOM implementation which will directly impact their ability to work with commercial companies that support federal information technology environments.

---

[3] https://csrc.nist.gov/projects/risk-management/about-rmf

[4] https://www.cisa.gov/uscert/sites/default/files/publications/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF

[5] https://www.cisa.gov/binding-operational-directive-22-01

[6] A non-exploitable vulnerability, based on NIST's use of the Common Vulnerability Scoring System (CVSS), means that there is no viable access vector, the access complexity level is exceedingly high, or the means of authentication prevents access to the vulnerability.

[7] https://www.cisa.gov/sbom

[8] As required in The Executive Order on Improving the Nation's Cybersecurity, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Ultimately, SBOMs will not achieve the desired utility for agencies at this point because of a lack of standardization. DHS's recent Cyber Safety Review Board review of the December 2021 Log4j event notes that SBOMs are currently limited, with differences in field descriptions and lacking version information.[9] This highlights the need for additional work to include guidance on the structure and construction of an SBOM and standardization of the processes for SBOM dissemination, ingestion, and use. Each of these is critical for sellers to create usable SBOMs and for government and other buyers to make effective use of the output.

We also urge the Senate to take these considerations into effect in its own upcoming NDAA bill and ensure alignment between guidance for federal civilian and defense agencies. It is critical that government and industry come together to create the best possible outcomes to improve supply chain security.

We strongly urge the Senate Armed Services Committee and the Senate Homeland Security and Governmental Affairs Committee to remove the SBOM language from the NDAA and give industry and agencies more time to develop solutions that will better secure the country's cybersecurity supply chain. We will continue to work with the House, Senate, and administration officials to mature SBOMs and improve the nation's security.

Sincerely,

Alliance for Digital Innovation

BSA | The Software Alliance

Cybersecurity Coalition

Information Technology Industry Association

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