



August 27, 2026

The Honorable John Thune
Majority Leader
U.S. Senate
Washington, DC 20510

The Honorable Mike Johnson
Speaker
U.S. House of Representatives
Washington, DC 20515

The Honorable Roger Wicker
Chairman
Senate Armed Services Committee
U.S. Senate
Washington, DC 20510

The Honorable Mike Rogers
Chairman
House Armed Services Committee
U.S. House of Representatives
Washington, DC 20515

The Honorable Chuck Schumer
Minority Leader
U.S. Senate
Washington, DC 20510

The Honorable Hakeem Jeffries
Minority Leader
U.S. House of Representatives
Washington, DC 20515

The Honorable Jack Reed
Ranking Member
Senate Armed Services Committee
U.S. Senate
Washington, DC 20510

The Honorable Adam Smith
Ranking Member
House Armed Services Committee
U.S. House of Representatives
Washington, DC 20515

Dear Majority Leader Thune, Minority Leader Schumer, Speaker Johnson, Minority Leader Jeffries, Chairman Wicker, Ranking Member Reed, Chairman Rogers, and Ranking Member Smith:

On behalf of the Business Software Alliance (BSA), we write to highlight key issues under consideration as the House and Senate work to reconcile their respective versions of the FY27 National Defense Authorization Act (NDAA). We appreciate your leadership in advancing this legislation and urge careful attention to provisions that impact the enterprise software industry, digital modernization, and the Department's operational readiness.

BSA represents the global enterprise software sector, whose innovations underpin U.S. competitiveness in cybersecurity, cloud infrastructure, data analytics, artificial intelligence (AI), and supply chain resilience.¹ We are encouraged that Congress recognizes the value of commercial

¹ BSA's members include: Adobe, Alteryx, Amadeus, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., TrendAI, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

technology in modernizing the Department securely and effectively and ensuring the Department can modernize with secure, effective tools.

Commercial Acquisition Reform and Business Systems Modernization

We strongly support provisions in the House bill that streamline commercial acquisition and reduce unnecessary contracting barriers for industry. In particular:

- **House Sec. 803:** Prohibits duplicative, DoD-unique contract clauses for commercial products and services beyond existing FAR/DFARS requirements.
- **House Sec. 807:** Codifies uniform data standards for electronic contract writing and acquisition management systems, with a commercial-first preference.
- **House Sec. 830:** Establishes permanent, government-wide authority to acquire services through consumption-based, usage-billed solutions.
- **House Sec. 851:** Directs a dedicated team to work down the backlog of open DFARS cases, with monthly briefings until resolved.
- **Senate Sec. 814:** Restricts DoD's centralized commercial item determination capability to prevent overly broad non-commercial determinations that disadvantage commercial vendors.
- **Senate Sec. 1637:** Directs the Secretary to ensure competitive procurement practices for advanced computing systems, AI applications, cloud computing, data infrastructure, and foundation models, including safeguards against vendor lock-in.

Modernizing IT Infrastructure and Cloud Capabilities

BSA welcomes continued attention in both chambers to cloud modernization, authorization-to-operate (ATO) reform, and the reduction of technical debt.

- **House Sec. 518:** Directs the Army to run a three-year pilot building a unified digital identity and integrated services platform for soldiers, recruits, and veterans across the service lifecycle.
- **Rules Committee Print 119-33, Amendment #800, Offered by Rep. Walkinshaw:** Establishes a FedRAMP high reciprocity pilot for DoD cloud security requirements.
- **Rules Committee Print 119-33, Amendment #1209, Offered by Mr. Moore of Utah:** Requires DoD to designate senior officials responsible for improving service delivery to servicemembers and their families, with a report to Congress within 180 days.
- **Senate Sec. 1623:** Directs a study on the feasibility and security implications of expanding SaaS adoption within classified DoD networks.
- **Senate Sec. 1624:** Requires DoD to reform and expedite the governance process for cross-domain solution approvals, reducing duplicative reviews.

Artificial Intelligence

AI continues to represent a critical area for national security innovation, and BSA supports measures that accelerate secure, competitive AI adoption within the Department.

- **House Sec. 1521:** Reforms software planning, programming, budgeting, and execution. This is an area that BSA has long advocated for modernizing.
- **House Sec. 1523:** Establishes a framework to accelerate deployment of AI models within the Department. BSA supports this language, and we ask that conferees ensure alignment with commercial AI acquisition preferences.
- **Senate Sec. 1646:** Requires the DoD generative AI platform to include alternative AI models beyond the initial selections, promoting competition and access for commercial AI vendors.

Cybersecurity, Quantum, and Post-Quantum Cryptography

We applaud provisions in both chambers that strengthen cybersecurity alignment, accelerate the transition to post-quantum cryptography, and improve quantum readiness.

- **House Sec. 1507:** Requires covered contractors to implement a vulnerability disclosure policy consistent with NIST guidelines, with FAR Council follow-through and CIO waiver authority. BSA supports this language that aligns cyber requirements to NIST and international standards.
- **House Sec. 1706:** Reauthorizes the bipartisan Cybersecurity Information Sharing Act of 2015 (CISA 2015) until 2035. The Act provides the foundation for industry and government to efficiently share cyber threat information.
- **Rules Committee Print 119-33, Amendment #1175, Offered by Reps. Moore and Harrigan:** Establishes an Army Quantum Readiness and Advanced Computing Initiative.
- **Senate Sec. 1631:** Mandates that DoD cryptographic solutions adopt NIST-approved post-quantum algorithms for key establishment by December 31, 2030, and for digital signatures by December 31, 2031.
- **Senate Amendment 6664 (Young):** Comprehensively reauthorizes and modernizes the National Quantum Initiative through 2034, expanding DOE/NIST/NSF/NASA quantum R&D and adding a post-quantum cryptography upgrade strategy.

Hardware Supply Chain and Printed Circuit Boards (PCB)

Current law at 10 U.S.C. § 4873 prohibits the Department from acquiring covered printed circuit boards from covered nations, but the definition does not explicitly exclude commercial products and services, and the commercial-exception rulemaking is discretionary rather than mandatory. The FY21 NDAA required that the DFARS include regulatory language to be effective on January 1, 2027. However, the rulemaking started on July 2, 2026—over 5 years from the passage of the original

language without any prior rulemaking process. This timing does not allow companies to update their supply chains in time for implementation, even as hardware needs have skyrocketed with the rapid growth of AI.

Neither the House nor Senate bill as currently drafted addresses this gap, but there are two provisions in the Senate bill, which raise related issues:

- **Senate Sec. 811:** Consolidates multiple existing commodity-specific foreign procurement restrictions into a new unified statutory framework under Title 10, explicitly including printed circuit boards alongside chemicals, munitions, telecom equipment, batteries, with an effective date of January 1, 2028.

- **Senate Sec. 844:** Expands the existing printed circuit board procurement restriction under 10 U.S.C. § 4873 to cover upstream precursor materials including copper clad laminate, copper foil, and glass, raising supply chain compliance concerns for contractors sourcing commodity inputs with heavily China-dependent global supply chains, with an effective date of January 1, 2029.

Given that this language is now present in the Senate bill, we ask that 10 U.S.C. § 4873 be updated to narrow the covered printed circuit board definition, explicitly excluding commercial products, commercial services, and COTS items, and adding a standalone “defense security system” definition. The update should also convert the commercial-exception rulemaking from discretionary to mandatory and add a rule of construction limiting certification requirements on commercial and COTS items. Finally, it would allow for the rulemaking process to finish with enough time that companies can update their supply chains in a rational manner. BSA urges conferees to adopt this additional language in the final bill.

Provisions of Concern

While BSA supports Congress’ continued focus on strengthening IT practices across the Department and the broader federal government, BSA members want to raise concerns about one Senate provision and three House floor amendments.

- **Rules Committee Print 119-33, Amendment #98, Offered by Rep. Nehls:** Would require the Department to review existing programs and implement software-based cryptographic protections in place of hardware-based approaches. While intended to advance the Department’s post-quantum transition and reduce vendor lock-in, the provision as drafted uses non-standard cryptographic parameters that conflict with commercial cloud key-management architectures, raises IP disclosure risks for vendors, and embeds procurement terms within what is framed as a security mandate. BSA opposes this provision and asks that conferees not include it in the final bill.

- **Rules Committee Print 119-33, Amendment #464, Offered by Rep. Ogles:** Bars DoD contracts with providers that give advance vulnerability disclosure to countries-of-concern entities. Coordinated vulnerability disclosure is a standard commercial software and hardware security practice, and this provision could be read broadly enough to capture routine practices rather than

only adversary-facing ones. BSA opposes this provision and asks that conferees not include it in the final bill.

- Rules Committee Print 119-33, Amendment #647, Offered by Rep. Begich: Adds a 72-hour reporting deadline for discovering Chinese-linked hardware, software, or firmware in covered contractor networks, layered onto existing cyber incident reporting requirements. BSA opposes this provision as currently drafted and asks that conferees not include it in the final bill.

- Senate Section 815: Bars any Pentagon contractor, regardless of contract size, from buying back stock or paying dividends for the life of the contract absent a waiver. This sweeping language includes partnerships, pass-through entities, and ESOPs, in addition to corporations that rely on dividends. BSA opposes this language as federal interference with corporate structures will hurt investors and could discourage private-sector participation in the defense industrial base.

Conclusion

Thank you for your leadership in advancing this year's NDAA. These provisions will determine how effectively the Department can leverage commercial innovation, strengthen IT infrastructure, and responsibly harness AI and quantum technologies. We stand ready to work with you and your staff to refine these provisions and ensure a strong, future-ready NDAA.

Sincerely,

Victoria A. Espinel