Business Software Alliance

February 11, 2026

The Honorable Roger Wicker
Chairman
US Senate Armed Services Committee
Washington, DC 20510

The Honorable Jack Reed
Ranking Member
US Senate Armed Services Committee
Washington, DC 20510

The Honorable Mike Rogers
Chairman
US House Armed Services Committee
Washington, DC 20515

The Honorable Adam Smith
Ranking Member
US House Armed Services Committee
Washington, DC 20515

Dear Chairman Wicker, Ranking Member Reed, Chairman Rogers, and Ranking Member Smith:

As you work to help the nation confront growing challenges through the Fiscal Year 2027 National Defense Authorization Act (FY27 NDAA), I write to offer the perspective of the enterprise software industry on key efforts that would improve our national and economic security and increase the Department of Defense's ability to accomplish its missions today and into the future.

The Business Software Alliance (BSA) is the leading advocate for the global enterprise software industry.[1] We work in over 20 markets in the Americas, Europe, and Asia, advocating for policies that build trust in technology so that the government, every industry sector, and the public can benefit from innovation.[2] BSA members are at the forefront of providing AI, cybersecurity, cloud computing, quantum, and other cutting-edge technologies.

The Department is both the US Government's leading innovator of security technologies, while also the largest in budget. It is well positioned to improve supply chain security, acquisition policy, cloud migration and use, research and development, capacity building and international leadership, and the nation's technology workforce.

We are eager to work with you to ensure that Congress and the Department leverage this opportunity and craft policies that simultaneously advance security, innovation, and competitiveness. To that end, we wish to share with you BSA's priorities for the FY27 NDAA that focus on commercial technology, IT modernization, reducing regulatory burdens, cybersecurity, and quantum technology.

---

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

[2] *See* BSA | The Software Alliance, Artificial Intelligence in Every Sector, *available at* https://www.bsa.org/files/policy-filings/06132022bsaaieverysector.pdf.

Victoria A. Espinel
CEO

200 Massachusetts Avenue, NW Suite 310 Washington, DC 20001
202.872.5500 **www.bsa.org**

1. Increased Use of Commercial Technology

The Department has often experienced cost overruns and performance issues when it has sought to develop custom-built software to address functions that readily available commercial-off-the-shelf (COTS) solutions can already provide. For many Department use cases, a COTS solution offers the best state-of-the-art solution, quicker time-to-mission, and at lower cost than custom-built software.

A. Comptroller General Review of the Commerciality of Defense Business Systems

COTS solutions offer current commercial capabilities with faster implementation and increased integration with other commercial software. 10 U.S.C. 2222 establishes a preference for the Department to use commercial business systems. To maximize the value of this provision, a GAO review to identify, which defense business systems are commercial, and which are custom built will provide data to inform a conversation for future modernization in line with US law, regulation, and policy.

B. Comptroller General Review of Commercial Technology to Support Contested Logistics

The Department and military services have made significant investments in hardware and defense business systems. Maximizing the use of modern commercial systems already available within the Department would align with the focus on speed, cost reduction, and use of commercial best practices. BSA requests that the Committees require the GAO review how the Department and military services should maximize the use of procured commercial business systems such as finance and logistics to improve the Department's capability of operating in contested logistics environments instead of procuring alternative solutions, which offer similar capabilities.

2. Modernize IT

To help address threats from geopolitical adversaries, the US Government needs to modernize the software that is currently being used across the Department and across the federal government. This is a whole-of-government issue as there are many Department and civilian agency systems that are still using COBOL—a fifty-year old coding language—for support systems. This use introduces cyber risk, while ignoring all the improved capabilities within modern commercial software. including advanced AI and agentic capabilities to enhance execution of the Department's mission.

One way to improve the overall health of federal IT is to leverage the panoply of cloud solutions that foster innovation and reduce the Government's total cost of acquisition. Infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) have proven to be effective and efficient ways to upgrade federal information technology. Currently, however, guidance promoting these solutions, particularly in connection with multi-cloud solutions, is lacking.

Cloud computing affords agencies access to innovation and the technological flexibility necessary to address mission requirements. Cloud computing offers access to more cost-effective, functional, and proven software solutions. At a base level, it allows users to access all the features and files of their systems without the need to lock-in to technology that will need upgrading over time, or to maintain local data storage resources. Cloud computing also provides agencies with access to unique, market-driven partnering relationships associated with the delivery of services. For instance, IaaS and PaaS providers can join their expertise with that of systems integrators to bring enhanced solutions to their customers. All told, these solutions promise cost reduction at a time when resources are in high demand.

Victoria A. Espinel
CEO

200 Massachusetts Avenue, NW Suite 310 Washington, DC 20001
202.872.5500 **www.bsa.org**

Multi-cloud solutions enhance the beneficial effects of cloud computing (improved cybersecurity, resiliency, redundancy, and access to artificial intelligence enabled by cloud computing). They encourage cost competition, allow for diversified applications and solutions, and facilitate system interoperability, which can enhance resiliency. They also reduce the risk of vendor lock-in created by the concentration of government data in one CSP cloud. BSA encourages the Committees to direct the Department to leverage cloud solutions to the greatest extent possible, particularly through the programs and recommendations below.

A. Information on Progress of Joint Warfighter Cloud Capability Program

BSA supports the Department's efforts to expand the cloud capabilities across the services. BSA supports the competition between Joint Warfighter Cloud Capability (JWCC) awardees and wants to make sure that the marketplace is vibrant. We applaud the Committees' efforts to advocate for good reporting through the FY25 NDAA bill. BSA requests that the Congressional reporting be publicly available to allow for a competitive landscape in the market.

B. Create a Working Capital Fund to Address Technical Debt

BSA supports the Pentagon's efforts to increase the effectiveness of IT systems throughout the Department. Given that there is a need to move data at the speed of the warfighter, there needs to be concurrent efforts to update the information systems that will enable the data to be used by AI and quantum programs. To facilitate the rapid digital transformation of US warfighting capability in line with the Artificial Intelligence Acceleration Strategy, Congress should authorize the creation of a permanent Services Information Technology Working Capital Fund. BSA asks the Committees to create a fund that would enhance the availability of "no-year" funds necessary for experimentation and adoption of frontier capabilities and AI within each service.

C. Guidance to Reduce Hardware and Software Technical Debt

BSA has long supported the efforts that the Department is focused on modernization. BSA commends the Committees' and the Department's efforts to reduce the technical debt that is slowing the use of modern IT and software that was included in the FY26 NDAA, particularly section 1503. This is an effort that requires a whole-of-government approach to be successful. BSA asks that the same emphasis on technical debt is extended to the civilian government so that the federal CIO will issue a guiding framework to track, assess, reduce, and manage technical debt in hardware and software systems.

D. Review of Defense Finance and Accounting Service Payroll Modernization

BSA has long advocated for modern systems that affect all government, whether payroll, human resources, contracting, or financial management. Many of these systems are in varying states of disrepair and face distinct challenges in transition to modern solutions. To address one of these issues, BSA requests that the Department's Chief Information Officer, which has purview over defense business Systems, and the Department of Defense Comptroller to jointly review the status of the Defense Finance and Accounting Service's efforts to modernize its payroll systems with current commercial solutions.

E. Aligning Data Center Policy with Commercial Cloud Requirements

BSA encourages the Committees to direct the Department to inventory the condition, utilization, and mission alignment of these facilities and to assess options for allowing commercial cloud providers to deploy advanced computing infrastructure—such as graphics processing units—within Department-owned environments. This would enable faster access to scalable AI capabilities while maintaining appropriate government control of facilities and security requirements. Such an approach could help mitigate capacity constraints, reduce time to deployment for AI enabled systems, and maximize the

value of prior federal investments in physical infrastructure, while ensuring compliance with Department cybersecurity, data protection, and national security standards. BSA members urge the Committees to develop a report that would examine contracting authorities and policy barriers to these partnerships that would further support the Department's ability to responsibly adopt cutting-edge commercial capabilities in support of warfighting and national security missions.

3. Limiting Regulatory Burdens

Disjointed regulatory requirements hinder the rapid adoption of AI and emerging technologies by increasing compliance complexity and slowing access to innovative solutions critical to the federal government. The information and communications technology (ICT) supply chain confronts significant security threats from both government and non-government actors. These threats implicate the Department's acquisition of ICT products and services. In response to these threats Congress and the Administration have launched multiple workstreams, but it remains unclear to industry whether and how these regulatory workstreams are coordinated or complementary.

Conflicting regulations can cause the industrial base to shrink as there are fewer new entrants that want to create individual programs for individual agencies or departments. As technology is moving, and it can take four years to get from concept to delivery in the Department[3],the need to reduce the burden and increase speed is critical. To leverage the potential of AI, BSA urges that the Department work in concert with the entirety of the federal government to determine harmonized regulations across the market.

4. Speeding the ATO Process

BSA has been active asking the Committees and the Pentagon to increase Authority to Operate (ATO)s across both the Department and the federal government. The Department also made progress toward reform and acceleration of the acquisition, testing, and authorization of secure software through the Software Fast Track (SWFT) Initiative. BSA requests the Committees' continued focus on translating any progress made by SWFT into enduring solutions. As an association representing industry leaders in cybersecurity and supply chain risk management, BSA continues to support the Department's goal of improving cybersecurity and supply chain risk management.

A. Increase Use of ATOs Across the Department and the Federal Government

The Committees encouraged the Department to use ATOs granted by one department across all departments. This allows for speed of use of new technologies across the Department. BSA appreciates the continued emphasis that the Committees placed on ATO through both the FY25 and FY26 bills. As this program is simplified, it will allow the Department to move at the speed of necessity to focus on the current technology problems. To further increase momentum, BSA suggests the development of a Cloud Security Reciprocity Pilot Program. This program directs the Department CIO to establish a cloud security authorization reciprocity pilot program to select a number of cybersecurity solutions authorized at FedRAMP High and perform an accelerated assessment to validate them for CC SRG Impact Level 5 and then assess the feasibility of expanding the number of participating solutions in the pilot program.

[3] U.S. Senate Committee on Armed Services. (2025, January 28). To receive testimony on defense innovation and acquisition reform. Retrieved from https://www.armed-services.senate.gov/hearings/to-receive-testimony-on-defense-innovation-and-acquisition-reform

B. Accelerating Cloud Security Authorizations

Given the need for fast implementation of commercial software, BSA continues to look for opportunities to increase the speed of authorizations and use throughout the Pentagon. BSA asks the Committees to direct the Department to submit a plan to reduce security assessment and authorization timelines for cloud services, including target reductions in authorization timelines and the feasibility of a provisional authorization pathway to permit assessment without a mission owner sponsor.

C. Simplify the ATO Process Across the Federal Government

Additionally, the US Government must prioritize reforming and simplifying the ATO process. A streamlined ATO procedure will accelerate the deployment of AI solutions to government users. Simplifying documentation requirements and enhancing support for AI providers during ATO package submission would significantly expedite the adoption of innovative technologies critical for national security and operational efficacy. BSA requests that the Committees work to require the use of an agency ATO be used across government without additional, duplicative submissions at subsequent agencies.

5. Cybersecurity

A. Post-Quantum Cryptography Readiness

BSA thanks the Committees for their focus on the Post-Quantum Cryptography (PQC) report language in the FY26 bill that recognized that future quantum computers will be able to break today's most widely used cryptographic algorithms. The next step in this urgent area is to make sure that the Department prioritizes the assessment and acquisition of commercially available automated quantum readiness capabilities. This will ensure that the Department is able to meet its new, accelerated 2030 PQC deadlines and address the immediate risks of Harvest Now, Decrypt Later attacks.

B. Deterrence Against Cyber Attacks on Critical Infrastructure

BSA members want to work with the Department to address threats from persistent cyber actors. Language in the Senate FY26 NDAA required the Pentagon to evaluate the full range of options to impose costs on adversaries that conduct malicious cyber activity. It also required interim and final briefings to the congressional defense committees by March 1, 2026 and June 1, 2026. This language will help establish an effective framework to prevent, discourage, and respond to hostile cyber operations against defense systems and will strengthen both national and economic security. BSA urges the Committees to include the prior Senate provision Section 1603, which will direct the Department to develop a strategy to deter cyberattacks targeting United States defense infrastructure.

C. Advance Zero Trust Architecture Across the Department

As cyber threats grow in scale and sophistication, the Department must accelerate its transition to a Zero Trust security model to safeguard critical missions and data. Zero Trust—anchored in continuous authentication, least privilege access, and real-time monitoring—provides a modern framework far more resilient than legacy perimeter defenses. Modern platforms that connect identity, endpoint, data, and network protections through automated policy enforcement will deliver consistent, scalable security. Clear requirements, milestones, and reporting will ensure steady progress and give personnel secure, seamless access to the systems on which they rely. To strengthen mission readiness, we urge the Committees to direct the Pentagon to prioritize Department-wide deployment of commercial, standards-aligned Zero Trust capabilities that integrate cloud-based identity management, automated threat detection, and unified security telemetry.

D. Map Cybersecurity Requirements to International or NIST Standards

BSA appreciates the Committees' continued commitment to improving cybersecurity. To enhance cybersecurity, improve the effectiveness and efficiency of the US Government, set the nation on a path for sustained growth, and better serve the American people, BSA urges the Committees to align with international or National Institute of Standards and Technology (NIST) standards. This will enable regulatory harmonization; improve access to innovative security solutions; and ease the strain on a cyber workforce already at overcapacity. BSA urges the Committee to include a requirement that agencies map new and existing cybersecurity requirements to existing internationally recognized standards or guidelines.

E. Increase Cyber Workforce Education and Opportunities

There are approximately 500,000 open cyber jobs across the US in public and private sectors, and for the sake of our national security, these jobs must be filled. Congress should leverage the NIST Workforce Framework for Cybersecurity to identify the areas of greatest need to government agencies and American businesses and then drive the demand for cyber training and education for workers, including entry-level workers and career changers, as well as those not pursuing four-year degrees through incentives (e.g., scholarships and tuition reimbursement) and the supply of training and education by leveraging America's two-year colleges. BSA recommends the Committee include programs that help prepare Americans to quickly fill open cybersecurity jobs.

# # # #

We would welcome the opportunity to work with you and your staff to address these ideas in the FY27 NDAA. Working together, we can forge a deeper partnership between Congress, the Department, and the enterprise software industry to advance national security and continue our digital transformation.

Thank you for your leadership, and we look forward to working with you.

Sincerely,

Victoria A. Espinel
President and CEO

Victoria A. Espinel
CEO

200 Massachusetts Avenue, NW Suite 310 Washington, DC 20001
202.872.5500 **www.bsa.org**