



March 4, 2024

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

The Honorable Roger Wicker
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 Reed, Ranking Member Wicker, Chairman Rogers, and Ranking Member Smith:

As you work to help the nation confront growing challenges through the Fiscal Year 2025 National Defense Authorization Act (FY25 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.

BSA | The Software Alliance¹ is the leading advocate for the global enterprise software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, providing the products and services that power governments and businesses. BSA members are also leaders in security, having pioneered many of the software security best practices used throughout the industry today.

The Department of Defense (DoD or Department) is both the US Government's largest department and leading innovator of security technologies. The DoD is therefore 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 DoD 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 FY25 NDAA.

1. Harness Cloud Services

To help address threats from geopolitical adversaries, the US Government needs 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

¹ BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Okta, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

proven to be an effective and efficient way 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 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.

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 Committee to direct the Department to leverage cloud solutions to the greatest extent possible, particularly through the programs and recommendations below.

A. Expansion and Oversight of Multi-Cloud Technology Throughout the Federal Government

To provide value for taxpayer money while delivering better service, federal agencies should choose the best cloud solution for the best price for a given workload. However, while some federal agencies have matured to adopt the multi-cloud approach to run efficiently and effectively, many are not following this commercial best practice. Multi-cloud allows for the best market solution for each application/workload to meet mission needs at the best price. Instead, many agencies award long-term, agency-wide, “winner-take-all” cloud platform contracts to a single provider. In doing so, agencies limit themselves to the innovation and solution of just one cloud platform provider, even while the industry is developing innovative solutions across a variety of platforms. This single-cloud practice limits the Government’s access to the best technology for a workload.

Additionally, having only one provider available for an agency eliminates any price competition for each workload. Long-term, “winner-take-all” contracts to a single provider encourage protracted award protests, as vendors fear being locked out of all cloud platform business with a particular agency in the future. Multi-cloud technology is the leading practice in the private sector, and the federal Government has the opportunity to move to this commercial practice to achieve its artificial intelligence and IT modernization goals. BSA requests that the committee include S. 2871, the Multi-Cloud Innovation & Advancement Act of 2023 into the FY25 NDAA.

B. 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. BSA requests that the DoD continue to focus on the adoption of commercial cloud technology through program award and notify Congress semi-annually of any sole source task orders that are awarded under the JWCC.

C. Direct DISA to Expedite Certification and On-Boarding of Cloud Service Providers (CSP) for Implementation of JWCC Program

BSA was pleased to see DoD award the JWCC in December 2022 as it supports the Committees’ preference for multi-cloud architecture that provides global accessibility, resilient services, commercial parity, fortified security, and competition. To maximize competition and assure resiliency, DoD must have access to all the leading CSP offerings. BSA notes that each service and Defense Agency is most often using a “cloud broker” model to enable access to these CSP’s. BSA is concerned that not all of the JWCC awardees are fully onboarded and available to the Department for competition. BSA asks that the Committees direct the DoD Chief Information Officer to provide a report and briefing to the Committees.

D. Bill Language Request Directing DoD to Require Specific Acquisition Planning for Data Use and Storage

As the cloud is being rolled out throughout DoD acquisitions, there is an increasing need for the acquisition workforce to make sure that they understand and account for software hosting requirements. Sound acquisition planning is a key determinant in successful procurement and a sound acquisition plan starts with data. Specifically, Congress should include bill language that requires acquisition professionals to document their thoughtful consideration as to how data is stored, accessed, and used to maximize efficiency, cost savings, and military readiness. Such documentation can be used to ensure compliance with DoD policies, enhanced oversight, and the establishment of best practices. BSA requests bill language directing DoD to require specific acquisition planning for data use and storage.

E. Direct DoD to Report on Efforts to Incorporate Cloud Native Application Protection Into JWCC

With cloud infrastructure adoption accelerating at a rapid pace, CIOs must be vigilant of the new threat vectors, expanded attack surface, and the additional security data monitoring workload that comes with securing new cloud infrastructure. Planning ahead for cloud security by adopting cutting edge, DoD-network-authorized Cloud Native Application Protection Platforms (CNAPP) will ensure DoD's cloud infrastructure can efficiently and effectively serve the warfighter without taking on unintended cybersecurity risk. DoD must pair its multi-cloud migration with effective cloud native security solutions that secure applications by design; ensure DoD network defenders maintain continuous visibility and control over cloud-centric misconfigurations, privileges, data, and vulnerabilities; and provide continuous, real-time protection for cloud workloads, applications, and APIs, regardless of network location. To this effort, BSA requests that the Committee ask the DoD CIO to report on efforts on the incorporation of cloud native application protection into the JWCC program.

2. Limiting Regulatory Burdens

The information and communications technology (ICT) supply chain confronts significant security threats from both government and non-government actors. These threats implicate the DoD'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. In order 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 market.

3. Speeding the ATO Process - Cybersecurity Maturity Model Certification (CMMC) and Federal Risk and Authorization Management Program (FedRAMP)

On December 26, 2023, the DoD announced CMMC 2.0 with an updated program structure designed to achieve the DoD's cybersecurity goals. As the comment period closed on February 26, there are a number of regulatory changes going on through the process, including CMMC and FedRAMP. 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. Harmonization of CMMC with Other Government-wide Related IT efforts and Internationally Recognized Standards

The Department has indicated its intention to align the CMMC with other federal and internationally recognized cybersecurity and supply chain security requirements (such as the Federal Risk and Authorization Management Program (FedRAMP) and ISO 27001) to the greatest extent possible to reduce or eliminate duplication. In many circumstances, companies that have obtained these certifications already surpass the vast majority of the CMMC's control requirements. Allowing for reciprocity with other cybersecurity requirements will reduce cost and administrative burdens while,

importantly, still enabling DoD to achieve its cybersecurity goals. In fact, allowing reciprocity will likely expedite DoD achieving these goals. BSA commends DoD for this commitment, and BSA urges the Committee to require DoD to produce reciprocity agreements and mappings to FedRAMP, ISO, and other appropriate certification schemes that achieve DoD's goals, prior to requiring companies to undergo unnecessary or duplicative certifications.

B. Increase FedRAMP ATO Process to Aid in Additional Cloud Services Adoption

FedRAMP has failed to reduce the duplication of efforts by commercial cloud providers to provide services to the federal government as it often takes 12 to 18 months for a new product review and 4 to 12 months for a Significant Change Request.

Current technology updates are pushed out on a quarterly or more frequent basis, so there is a conflict between the commercial market and the ability for the federal government to obtain current software. BSA believes that security and speed can reasonably co-exist. BSA asks that the Committees look to fund the FedRAMP PMO at a level to eliminate the current backlog in review and increase the tempo on the Significant Change Requests assessments. BSA also asks the Committee to request OMB to provide public reporting on the FedRAMP authorizations and the status of the requests so that the DoD can use FedRAMP as a part of the CMMC process and eliminate burdensome and lengthy audits for Level 2 CMMC.

C. Increase Use of ATOs Across the DOD and Across the Federal Government

The Committee encouraged the DoD to use ATOs granted by one department across all departments in the DoD. This allows for speed of use of new technologies across the DoD. BSA urges the Committees to ask the DoD CIO for a report on the use of cross DoD ATOs and those instances where multiple ATOs for the same software were required in one year from the date of bill enactment.

BSA members also note the request for multiple ATOs is an issue that works across the government. BSA asks that the Committees work to require the use of FedRAMP authorization as a per se ATO, without additional ATOs, government wide.

4. Improve Software Acquisition and Security

BSA is eager to see the Department continue to build on the Committee's work improving software acquisition practices. BSA believes additional steps would improve the Department's ability to harness the power of the most innovative, secure software available.

A. Improving the Security of Open-Source Software

BSA appreciates the Committee's concern about the origin of source code and security of software in use by the DoD, other national security agencies, the Federal Government broadly, and in particular, software that has been acquired or developed by the Department and not gone through normal acquisition channels. This concern includes the acquisition of free and open-source software (FOSS), which is routinely introduced for use by the Department or contractors and researchers working on behalf of the Department by downloading from online, open software code repositories.

BSA recommends that the Committee direct the Secretary of Defense, in coordination with the Under Secretary for Acquisition and Sustainment and Chief Information Officer, develop policies for FOSS acquisition that ensure the same standards of evaluation that currently apply to other external software acquisitions, including: legal license review and record retention for authorized usage and any modification; vulnerability and reputation assessments of the software and its developing organization(s) supply chain and developer community; compliance with existing NIST security standards; availability and designation of how and where to receive software support; availability of product lifecycle calendar for expected period of support, upgrades, and patches to maintain the software; availability of published security bulletins identifying known vulnerabilities and mitigations, including an automated notification

processes of security updates; and software asset management to record which systems are using the software.

B. Embracing Best-in-Class Commercial Solutions

DoD 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 DoD 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. In approaching software acquisition reform, BSA recommends the Committee establish a clear, mandatory preference for best-in-class COTS software where such software can meet the Department's requirements. BSA also recommends the Committee direct the Department to assess, develop a strategy for, and provide a report on opportunities to utilize commercial software to improve business operations and reduce operations costs for the Department.

This requirement should include, but not be limited to, modernization of enterprise resource planning and business process automation, which can be improved dramatically with the use of Platform as a Service (PaaS) and Software as a Service (SaaS) solutions that are available as COTS, and an expansion of the FAR 2.101 definition of COTS to include XaaS (or "anything as a service") offerings that are not sold as items of supply.

BSA recommends the Committee also direct a review of Department of Defense Instruction 5000.75 (Business Capability Acquisition Cycle), to determine whether its business capability acquisition rules align with the need for speed and agility, and whether the rules enable a competitive environment for innovative information technology and software solutions.

C. Expanding Security Information and Event Management Services to Sensitive CUI

Commercial off-the-shelf security information and event management (SIEM) is critical to network security. Such capability provides a single system that offers visibility into a customer's networks, allowing for real-time threat response. The increasing use of a SaaS model calls for security to remain a key consideration. To ensure the Department has access to the most effective services, BSA urges the Committee to explore expanding SIEM for higher sensitivity controlled unclassified information through a pilot program for COTS SIEM services for IL-5; report to the Committee on the program; and consider aligning with the security orchestration and automated response pilot activity that was directed in the FY2022 NDAA.

D. Modernizing Management Capabilities

Section 836 of the FY21 National Defense Authorization Act directed the Secretary of Defense to develop and integrate digital data management and analytical capabilities. While the Department's current use of the Advana platform serves as a baseline capability, commercial off-the-shelf data management software must be more incorporated.

As such, BSA recommends that the Committee direct the Secretary of the Department to integrate COTS products to the greatest extent practicable and to inform the Congressional defense committees of a plan for such incorporation. In any report or future funding request, the Secretary should include budget justification information associated with commercial off-the-shelf enterprise data management software.

E. Modernizing the DoD's Data Logging

With the ever-increasing cybersecurity threat to national security systems and defense networks, such as SolarWinds and Log4j, the Committee is concerned that the Department lacks an enterprise-wide standardized format for data logging. In August 2021, the Administration directed departments and agencies to implement a maturity model for event log management in OMB-21-31², in accordance with

² M-21-31 (whitehouse.gov)

the investigative and remediation capability enhancements contained in Executive Order 14028, Improving the Nation's Cybersecurity.³ However, the Department of Defense has largely ignored the requirements contained in OMB-21-31. Accordingly, BSA recommends that the Department submit to the defense committees a report on its implementation plan for OMB-21-31, including plans for the use of commercial-off-the-shelf solutions and to include associated funding for implementation with the Department's budget submission for FY2025.

5. Outbound Investment

As reflected in our September 2023 comments to the Treasury Department, BSA shares the US Government's goal of restricting investment that would accelerate the development of military, intelligence, surveillance, and cyber-enabled capabilities in countries of concern.

We ask the Committees to allow the Treasury Department to advance its regulatory program to restrict outbound investment before developing potentially duplicative or conflicting legislation. Treasury's advance regulations clearly define prohibited and notifiable technology categories. Past legislative proposals contained language that was ambiguous or overbroad. Some proposals sought to restrict activities across undefined industry sectors, making it harder for the United States to maintain visibility and access to overseas technology. That visibility is critical to ensure continued US technology leadership and to protect our national defense. BSA urges the Committees to allow the current regulatory process to proceed and to consider advancing relevant legislation at a later stage.

6. Fund Research and Development on AI


BSA appreciates the Committee's support of research and development (R&D) efforts at the Department, particularly basic and applied research into emerging technologies, such as artificial intelligence (AI), wireless communications networks, and quantum computing. BSA strongly supports robust investments in quantum computing and AI at the Department. Capitalizing on advances in these areas will depend on vibrant cross-disciplinary R&D, supported by basic and applied research programs across multiple topical areas. BSA strongly supports increases to AI and quantum research and encourages the Committee to prioritize funding for them while sustaining funding for the broader portfolio of basic and applied research. In addition, we encourage the Committee to support research into the development of software for quantum computers, with an emphasis on understanding how secure software development lifecycles will need to evolve for quantum computing environments.

#

We would welcome the opportunity to work with you and your staff to address these ideas in the FY25 NDAA. Working together, we can forge a deeper partnership between Congress, DoD, 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

³ Federal Register: Improving the Nation's Cybersecurity