September 12, 2024

The Honorable Chuck Schumer
Majority Leader
US Senate
Washington, DC 20510

The Honorable Mitch McConnell
Minority Leader
US Senate
Washington, DC 20510

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

Dear Majority Leader Schumer, Minority Leader McConnell, Chairman Reed, and Ranking Member Wicker:

On behalf of BSA | The Software Alliance, I would like to draw your attention to several important topics that will arise during the Senate's deliberations of S.4638 the National Defense Authorization Act (NDAA) for Fiscal Year 2025. We ask that you review the following recommendations about specific provisions included or that may be included in the final product for consideration later this year. We appreciate your leadership on this legislation as these topics impact many of our members and significantly affect the enterprise software industry and consequently both our government and business customers.

BSA is the leading trade association representing the global enterprise software and technology industry.[1] Digital transformation, and the software that enables it, is essential to businesses of all sizes and in every industry. Our members provide cutting-edge cloud services, data analytics, manufacturing and infrastructure tools, and other digital capabilities to help businesses modernize and grow.

The Department of Defense (DoD) is both the federal government's largest department and the leading innovator of security technologies. Our members are focused on supporting the DoD's (and other agencies') digital transformation, which means providing the products and services the DoD needs to complete its missions effectively and efficiently today and well into the future.

Earlier this year, we wrote to the Senate Armed Services Committee about our priorities for this year's legislation to advance multi-cloud technology, Artificial Intelligence, cybersecurity, and harness digital transformation at the DoD, and we are grateful that you addressed many of these priorities in the legislation. As the bill proceeds, we urge you to continue to attend to those and other priorities, addressed below.

As you will see, our recommendations address provisions already in S.4638 as well as amendments that have been filed in advance of floor consideration.

[1] BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Cohere, Databricks, DocuSign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, 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.

Victoria A. Espinel
President and CEO

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

Expansion and Oversight of Multi-Cloud Technology Throughout the DoD
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 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. 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 cloud service provider.

- Section 810 in S.4638 enables several positive outcomes for the Executive Branch as it seeks to promote artificial intelligence while also elevating the need for multi-cloud procurement. **BSA supports Sec. 810 to ensure competition in AI procurement while also creating the infrastructure for utilization of AI in the DoD.**

- 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. Public reporting will help to ensure competition across the contracts. **BSA supports Sec. 884 that requires public reporting on the task orders awarded under JWCC.**

- With cloud infrastructure adoption accelerating at a rapid pace, CIOs must be vigilant to the new threat vectors, expanded attack surface, and the additional security data monitoring workload that comes with securing new cloud infrastructure. Planning 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. **BSA supports Sec. 1612, which requires the DoD CIO to develop a strategy on JWCC to incorporate zero-trust, standardize user identities, and increase AI applications in the JWCC and other multi-cloud environments.**

- BSA supports the ongoing efforts by the Senate Homeland Security and Government Affairs Committee with the passage of S.2871, the Multi-Cloud Innovation and Advancement Act of 2023, out of committee. The benefits of using a multi-cloud architecture have been recognized by Congress, federal agencies, and leading companies around the world. We urge the committee to adopt this language as it has government-wide applicability. The bill **ensures that the federal government has the tools they need to make the best decisions on cloud technology, and BSA urges the inclusion of this language in the bill.**

- BSA appreciates the concern that the Committee has with international competition. However, the language in Senate Section 885: Phase-Out of Computers or Printers Acquisition involving Entitles Owned or Controlled by China is over-broad in scope and pulls in IT infrastructure beyond the intended scope. This language would require a graduated phase out of DoD acquisitions of printers and computers from Chinese entities. The schedule would mandate 10% non-China threshold in FY26, increasing to 95% non-China by 2029. As with the House provision from FY 24, "manufacturer" is broadly defined to include the entity that

Victoria A. Espinel
President and CEO
200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001
P 202-872-5500
W bsa.org

transforms components into an end item, and an entity that subcontracts the manufacturing to an entity in China or directs manufacturing in China. "Computers" are defined to include personal devices but also cloud based data storage facilities, defined as "data processing devices performing storage functions, including a data storage facility." **BSA urges the Senate to modify § 885 to clearly exclude cloud services from the scope and to modify the definition of manufacturer to carve out entities with a U.S. parent.**

Artificial Intelligence

BSA members are on the leading edge of providing artificial intelligence (AI)-enabled products and services. They are at the forefront of the responsible development of AI, providing trusted software solutions that enable enterprises to harness the power of the technology to improve their operations and services. They have unique insights into enterprise AI's tremendous potential to further spur digital transformation in the private and public sectors and the policies that can best support the responsible use of AI.

- As the need for digital transformation accelerates with the new technology, it is more important than ever to broaden opportunities, promote alternative paths, improve training programs, and expedite the development of the diverse workforce needed to secure our shared future. Section 231 in the NDAA requires DoD to identify and brief on the Department's AI workforce. **BSA believes that a strong workforce is imperative for DoD to successfully use AI and supports the continued inclusion of Section 231 in the Senate NDAA.**

- BSA strongly supports robust investments in quantum computing and AI at DoD. 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. Senate Amendment 2616 would establish the National Artificial Intelligence Research Resource (NAIRR). The NAIRR's goals are: spurring innovation and advancing the development of safe and trustworthy AI; improving access to AI resources for researchers and students; improving capacity for AI research in the U.S.; and supporting the testing, benchmarking, and evaluation of AI systems. **BSA supports Amendment 2616 and asks that it be included in the final Senate text.**

- BSA believes that improving the physical security and cyber security of advanced AI models is an important issue. Amendments 2857 and 3139 need further discussion with both relevant stakeholders and the applicable Congressional committees. BSA appreciates the focus on security but believes that the procedures may not bring the intended consequences. Amendment 2857 provides broad authorities to the Executive Branch by permitting the President to mandate undefined obligations on private sector firms based on a determination that an AI firm presents "national security, economic stability, or public safety risks." This amendment also waives the need for the Executive Branch to follow the Administrative Procedure Act. This process guides regulatory comment so that the Executive Branch must consider all stakeholder comments on the proposed creation, promulgation, and implementation of new, undefined, and potentially broad rules which could inadvertently negatively impact American firms.

  Amendment 3139 represents the same goal to improve physical and cybersecurity of advanced AI models. It also needs broad stakeholder consultation in addition to the relevant Congressional committees, as it is too important to miss that step in the process. This amendment creates directives to develop, and then implement, a framework for cybersecurity standards based on non-existent metrics and measurements aimed at quantifying concepts like "national security and economic stability." Much of this work is ongoing by the National Institute of Standards and Technology (NIST) and the US Artificial Intelligence Safety Institute. Congress is preempting ongoing work, and we ask that Congress allow that process to finish before creating new work streams. **BSA opposes Amendments 2857 and 3139 in the Senate's version of the NDAA.**

- BSA supports the ongoing bipartisan efforts to incorporate the NIST Risk Management Framework (RMF) as part of procurement for high-risk AI uses. This would help establish the US government as a market leader on responsible AI, embracing best practices for managing

Victoria A. Espinel
President and CEO
200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001
P 202-872-5500
W bsa.org

AI risks, and holding Federal contractors to the same standard. Applying the NIST RMF in the procurement context, as well as other contexts, can help companies large and small measure and manage AI risks.

Many AI systems will be deployed for low-risk uses, like helping individuals locate recently viewed electronic files or filtering out background noise on a video call. These sorts of low-risk uses can create benefits for users but do not require further accountability measures. But for high-risk uses, like decisions to deny someone housing, employment, credit, education, healthcare, insurance, or access to physical places of public accommodation, the NIST RMF provides an important tool for mitigating AI risks. **BSA asks the Senate to include Amendment 3013 in the final Senate bill.**

Quantum

- BSA believes that the emergence of quantum computers will create a technological leap forward. Both the federal government and industry are investing heavily and working diligently to tap the full potential. Section 243 calls for the Director of the Defense Advanced Research Projects Agency (DARPA) to establish an initiative to rapidly expand and support quantum computing capability for DOD. **BSA supports this critical effort outlined in Sec. 243 Quantum Scaling Initiative and calls for maintained inclusion in the bill.**

Outbound Investment and Export Controls

- BSA strongly supports security in cloud computing and is pleased to work with the Administration and Congress on a variety of efforts in this area. However, there is an amendment filed that seeks to make US cloud providers responsible for the data that their customers house in the cloud. Treating access to the cloud as a regulated export could have negative and wide-reaching impacts on multinational companies, including US companies and companies in partner countries, who rely on access to enterprise management software around the world.

  The amendment puts US cloud providers in an impossible position of having to cut off or restrict cloud access to customer content that they do not have visibility or a legal right to access. The amendment appears to presume that US cloud providers have direct access to information. To comply with the amendment, US cloud service providers may have to terminate customer access more broadly or demand access to highly sensitive content.

  This language also overrides years of legal practice. Historically, the Department of Commerce Bureau of Industry and Security (BIS) has taken the position that such a “cloud service” does not involve an export and therefore would not be subject to export control restrictions, starting in 2009 and continuing through the present.

  Finally, such a requirement would likely further create incentives for multinational businesses doing business in China and other countries to choose Chinese IAAS providers – producing an outcome that would further weaken US national security interests. **For these reasons, BSA asks you to oppose the inclusion of Amendment 2187 into the Senate’s version of the NDAA.**

Cybersecurity

- BSA applauds the Committee’s encouragement for 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 Committee to support the language in Section 1621.**
- BSA supports the effort to update the Federal Information Security Management Act of 2014 (FISMA) as the bill established guidelines and cybersecurity standards across the federal government. BSA has been working with the authorizing committees of jurisdiction to sharpen the bill text. We offer important improvements to the language below.

Victoria A. Espinel
President and CEO

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

First, BSA advocates that FISMA should be updated to use FedRAMP authorizations across the government in Section 118 below.

"(F) The assessment of security controls and materials within the authorization package for a FedRAMP authorization pursuant to chapter 36 of title 44, United States Code, shall be presumed adequate to fulfill the responsibilities of the head of an agency set forth in this paragraph (1) with respect to an agency authorization to operate cloud computing products and services.

(i) The presumption under paragraph (1) does not modify or alter—
(a) the responsibility of any agency to ensure compliance with subchapter II of chapter 35 of title 44, United States Code, for any cloud computing product or service used by the agency; or
(b) the authority of the head of any agency to make a determination that there is a demonstrable need for additional security requirements beyond the security requirements included in a FedRAMP authorization for a particular control implementation."

Second, BSA also advocates that a rule of construction is added to the base text. BSA advocates for federal agencies to use commercial products rather than federally developed software. The research and development cost for federal software is high as is the ongoing maintenance of it. Commercial software provides reliability, scalability, and flexibility so that agencies can nimbly respond to unexpected or changing conditions. It is also updated and upgraded to respond to the market, so if security patches are needed, they can be updated quickly. By including a rule of construction language below, the additional will help to clarify the preference for commercial products.

"Section 118 (h) RULE OF CONSTRUCTION.—Nothing in this section shall prevent an agency from using a commercially available product (as defined in section 103 of title 41) or commercial service (as defined in section 103a of title 41) that meets or exceeds the requirements of subparagraphs (C), (D), and (E) of subsection (f)(1)."

BSA supports the inclusion of the language above and urges the Senate to include the updated Amendment 2121 to the final bill.

Defense Contracting Provisions

- BSA members are concerned about the speed of federal procurement, which is not updating at the same rate of change that meets the speed of IT evolution. **We support Amendment 2878 that would improve Federal technology procurement, and we urge the Committee to include it in the final bill.**

Thank you for your time and consideration of the above-mentioned recommendations, and we would welcome the opportunity to work with you and your staff to address these priorities in the final version of the FY25 NDAA. Thank you for your leadership, and we look forward to working with you.

Sincerely,

Victoria A. Espinel

Victoria A. Espinel
President and CEO
200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001
P 202-872-5500
W bsa.org