October 20, 2022

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

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

The Honorable Nancy Pelosi
Speaker
US House of Representatives
Washington, DC 20515

The Honorable Kevin McCarthy
Minority Leader
US House of Representatives
Washington, DC 20515

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

The Honorable Jim Inhofe
Ranking Member
US Senate Armed Services Committee
Washington, DC 20510

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

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

Dear Majority Leader Schumer, Minority Leader McConnell, Speaker Pelosi, Minority Leader McCarthy, Chairman Reed, Ranking Member Inhofe, Chairman Smith, and Ranking Member Rogers:

On behalf of BSA | The Software Alliance, I would like to draw your attention to several important topics that will arise during the conference for the FY2023 National Defense Authorization Act (NDAA) and 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 impact 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. 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 software industry supports nearly 16 million US jobs, including 12.5 million outside the tech sector, and contributes $1.9 trillion to the US economy.

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 you about our priorities for this year's legislation to advance cybersecurity, drive agile and meaningful innovation, and harness digital transformation at the DoD, and we are grateful that you addressed many of these priorities in the legislation. As the conference committee proceeds, we urge you to continue to attend to those and other priorities, addressed below.

Victoria A. Espinel
President and CEO

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

Software Supply Chain Risk Management (SBOM)

- BSA supports the development and use of software bills of materials (SBOMs) as well as the associated tooling, standards, and automation necessary for transforming the information contained in an SBOM into concrete cybersecurity improvement. However, **BSA requests the committee strike section 6722 of the House bill.** It undermines the current progress among the software industry, government, and other stakeholders to develop SBOMs. Additionally, the OMB guidelines issued on September 14, 2022, requiring self-attestation from software vendors for federal use demonstrates the Administration thinks a more phased and nuanced approach to SBOMs requirement is appropriate at this stage. Finally, the language concerning the mitigation of all vulnerabilities is inconsistent with internationally recognized standards and best practices for security and current CISA guidelines for agencies, under which mitigation efforts are prioritized based on risk.

- Although we caution against the premature codification of SBOM that may undermine current implementation efforts, if the Committee sees fit to include work on SBOMs in the NDAA, BSA would suggest **refining the scope and definitions in the language involving SBOM's to section 1627 language of the Senate Bill** that directs the Department of Defense, "in consultation with industry, [to] develop an approach for commercial software in use by the Department and future acquisitions of commercial software that provides, to the maximum extent practicable, policies and processes for operationalizing software bills of materials," while aligning the definition of SBOMs used in that text to EO 14028 definition.

Federal Contracting for Peace and Security Act

- One of the amendments included in the House-passed version of the NDAA is a revised version of the "Federal Contracting for Peace and Security Act." Currently, there is no companion measure to this amendment in the Senate version. We appreciate the underlying intent of the amendment and understand the importance of ceasing and winding down operations in Russia. BSA members are doing so, and in many instances working with the Administration. In some cases, there are legal, policy, and security complications that are important to consider and address. The amendment leaves important questions unanswered of how it would work in practice and address unintended consequences. **BSA requests the conference to remove the language that was included in this amendment from the final version of the NDAA.**

Outbound Investment

- As reflected in BSA's report on Effective ICT Supply Chain Security, BSA endorses the need to manage supply chain security risk. However, we do not support the inclusion of the outbound investment screening framework in the NDAA. Proposals that broadly restrict activities across numerous undefined industry sectors could imperil US technology leadership by making it harder for US companies to maintain visibility and access to overseas technology that can be purchased or licensed to make US business and manufacturing operations more competitive. Because foreign competitors from the EU, Japan, Korea, and elsewhere would face no similar restraints, American companies would face a competitive disadvantage. Prior Senate legislative proposals have covered a much wider array of commercial activities than the type of equity or other investments that are currently addressed by the Committee on Foreign Investment in the United States (CFIUS). Furthermore, these legislative proposals have been overbroad in scope and industry coverage, capturing many sectors and technologies that are already commercially available around the world. For these reasons, any review mechanism should be scoped to focus strictly on actual investments in countries of concern relating to sensitive technologies the exportation of which is already controlled under US export control laws. Lastly, any such proposal should be subject to the regular process, including relevant committee review and hearings. **For these reasons, BSA asks you to oppose the inclusion of this issue in the NDAA of the overbroad discussion drafts that have been publicly evaluated to date.**

Victoria A. Espinel
President and CEO

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

Shop Safe

- BSA is concerned that the NDAA may include elements of the SHOP SAFE Act, a measure that attempts to limit counterfeit items sold through online marketplaces. BSA has a long history of advocating for strong IP protections against patent abuses and fraud. However, the SHOPE SAFE Act is flawed in several ways, most notably the overbroad definitions of "electronic commerce platform" and "goods that implicate health and safety" would sweep in a large swath of enterprise service providers beyond these marketplaces directed at American households, misplacing responsibility, and imposing source-intensive compliance burdens, not in the spirit of the measure. Further, the problems with the overbroad definitions would be compounded by SHOP SAFE's creation of a novel form of contributory liability that would expose business software providers that are far removed from any underlying infringement to expansive private litigation. **Therefore, BSA opposes the inclusion of elements of the SHOP SAFE Act in any final product of the NDAA**

Improving Intergovernmental Cooperation and Reducing Duplication Act

- BSA member companies strongly support the goal of ensuring state, local, tribal, and territorial (SLLT) governments have effective information technology (IT) to deliver resources and services to all Americans. However, we are concerned the NDAA may include language that encourages the DoD or other federal agencies to replicate IT solutions by developing its own technology to provide to SLLTs at a subsidized cost or without reimbursement, even when commercial and commercial off-the-shelf (COTS) products are available. This represents a break from the US government's longstanding policy of relying on private enterprises to innovate and provide IT services to the public sector. It will also likely result in SLLT having old, less functional, and potentially less secure IT in the future as the Federal Government has a track record of not keeping pace with the innovation that is a KEY of the private sector. **BSA member companies are concerned this policy would encourage the federal government to invest in developing and maintaining technology that can be provided through the private sector.**

***Federal Information Security Management Act (FISMA)* Reform.**

- BSA applauds the Senate's leadership in updating *Federal Cybersecurity Enhancement Act (FCEA)* authorities as part of a larger proposed revision to the *Federal Information Security Management Act* (FISMA) as filed as an amendment to the FY23 NDAA. BSA would have preferred that the Senate strike the blatantly monopolistic language in Section 5022, sub-paragraph (d) of sub-section (f)(1) that preferences a specific government-off-the-shelf technology. However, we applaud the "Rule of Construction" in sub-section (h) as vital to bringing needed clarity to improve vendor choice among Federal Civilian Executive Branch agency CIOs in procuring those commercially available digital identity solutions that meet or exceed the FCERA requirements. **BSA asks Leadership to insist on including the aforementioned "Rule of Construction" as drafted clarifying vendor choice at agencies should either FCEA or FISMA modernization language advance, whether as part of the FY23 NDAA or any other legislative vehicle this Congress.**

Strengthening Agency Management and Oversight of Software Assets Act (SAMOSA)

- Federal government agencies should be run efficiently and effectively. BSA | The Software Alliance Software believes that software is a key solution to achieving this goal. Without question, there is room for federal agencies to improve how they acquire, implement, and utilize software. However, the Strengthening Agency Management and Oversight of Software Assets Act (SAMOSA) does not support that objective. BSA and its members welcome a collaborative effort alongside staff to fully realize the purpose of the bill -- to ensure taxpayer savings and that those federal agencies continue to have the most cost-effective and effective products. **BSA Member companies request additional and meaningful input from all**

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

stakeholders and request this legislation or others addressing the procurement of software by federal agencies not be included in the NDAA or other legislation in 2022.

Addressing Section 889 of the National Defense Authorization Act for Fiscal Year 2019

- As written, Section 889 of the FY 2019 NDAA risks damaging numerous segments of the economy and requires significant waiver authority. Including semiconductors in this provision will only compound these issues and could inadvertently undermine potential progress to address shortfalls addressed by the CHIPS Act. The United States is currently at a disadvantage, and China is one of the most dominant producers. While we believe a three-year implementation period to the application of semiconductors to Section 889 is prudent **BSA and its member companies believe that until the long-term benefits of the CHIPS Act are realized, it is best to remove this amendment from the conference bill. At a minimum, BSA requests the language involving the** Federal Acquisition Supply Chain Security Act to be applied to semiconductors in the waiver process.

FedRAMP and the Reuse of Authorizations to Operate (ATO's)

- The FedRAMP was designed to accelerate the adoption of secure cloud solutions through the reuse of assessments and authorizations; establish a baseline set of agreed-upon standards for cloud product approval; ensure consistent application of security practices and improve monitoring. In practice, FedRAMP has struggled to meet its objectives based on the pace of change in security solutions, resourcing, and demands for review and authorizations. Numerous proposals both in the Department and outside have led to a disjointed approach across the government to cybersecurity.

  The problems are exacerbated by the limited reuse of authorizations to operate (ATOs). In sum, the rigor of the FedRAMP process is not being leveraged sufficiently by the Federal government, which delays access to cloud service providers that "have unique access to and insight into cyber threat and incident information." This result is directly counter to President Biden's May 12, 2021, Executive Order on Improving the Nation's Cybersecurity. Ultimately, ATO delays weaken the cyber industrial base, drive up costs for taxpayers, and place at risk government agencies from obtaining timely and secure cloud technology. **BSA recommends that Congress direct the Comptroller General to submit a report to the Armed Services Committees on how the rules for cybersecurity in procuring cloud services differ among agencies; how agencies are managing risk within their networks; whether ATOs are, or should be, accepted across agencies; how accreditation at DISA corresponds to FedRAMP and other security requirements; and the status of efforts to establish reciprocity among the various authorizing agencies**. The report should provide recommendations for centralizing the US government's cybersecurity posture to better coordinate among different certifications to meet modernization and security objectives.

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 FY23 NDAA. Thank you for your leadership, and we look forward to working with you.

Sincerely,

Victoria A. Espinel
President and CEO

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org