April 22, 2022

The Honorable Jack Reed
Chairman
The Honorable Jim Inhofe
Ranking Member
Senate Committee on Armed Services
SR-228 Russell Senate Office Building
Washington, DC 20510


Dear Chairman Reed and Ranking Member Inhofe:

As you work to help the Nation confront growing challenges through the Fiscal Year 2023 National Defense Authorization Act (FY23 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 Alliance[1] 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 FY23 NDAA.

## 1.      Ensure Supply Chain Security

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 supply chain security workstreams are coordinated or complementary.

---

[1] BSA's members include Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Prokon, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., 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

### A.  Creating a Strategic, Whole-of-Government Approach to Supply Chain Security

BSA urges the Committee to exercise its leadership in ensuring a strategic, whole-of-government approach to supply chain security risk management that takes an assurance-based approach.[2] An assurance-based approach would create incentives for companies to improve their supply chain risk management by adopting best practices. Further, risk-management is more nuanced and tailored to the current environment, and more agile to adapt to future threats, than the regulatory, interventionist approaches used over the last few years, which have been blunt instruments, challenging or impractical to implement, harmful to US industry, and all without ultimately improving risk management.

BSA expects the Committee will consider proposals for addressing ICT supply chain risks and urges the Committee to evaluate such proposals to ensure that supply chain security laws and policies: use assurance-based approaches; embrace internationally recognized, industry driven standards; utilize risk management approaches that prioritize security measures based on the most relevant and potentially impactful risks; remain transparent to the public and include notification mechanisms for impacted stakeholders and meaningful processes for resolving disputes; be enforceable, for example by establishing supply chain risk management responsibilities in vendor contracts; and support public-private collaboration.

### B.  Clarifying Section 889 of the Fiscal Year 2019 NDAA

In Section 889 of the FY19 NDAA, Congress sought to address supply chain concerns relating to five technology companies based in China. In subparagraph (a)(1)(B), Congress prohibited government contracts with companies that *use* any "covered telecommunications equipment and services." BSA supports the national security objectives of this section but has concerns with the implementing rules that apply more broadly than for national security. The prohibition may have legitimate security implications if the covered equipment is used in connection with the performance of a government contract, but it is counterproductive when applied to all unrelated uses.

The Federal Acquisition Regulatory (FAR) Council's interim rules applying this subsection appear to apply to any "use" of covered equipment, even if that use is limited to commercial activities bearing no connection to a federal contract. In addition, the FAR Council permits an exception for the Federal Government to enter into a contract for the provision of equipment from a covered provider that does not "route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles," but does not apply this exception to the *use* of the exact same equipment by a contractor. These rules do not appear to advance the national security objectives of this Committee.

BSA urges the Committee to clarify that subparagraph (a)(1)(B) applies only to use related to the performance of a government contract and that the exceptions permitted by the FAR Council apply to both subparagraph (a)(1)(B) and subparagraph (a)(1)(A).

The Department has a waiver from implementation of Section 889 until September 30, 2022. It is therefore important for this Committee to exercise oversight of the rules that are currently in force and apply across the Federal Government, and make appropriate amendments as suggested above.

### C.  Ensuring the Supply of Printed Circuit Boards

BSA continues to be concerned about the potential for Section 851 of the FY22 NDAA to further complicate the printed circuit board supply chain, and ultimately introduce more challenges to our national security. Section 851 of the FY22 NDAA restricts the sourcing of printed circuit boards, which do not have their own logic capabilities before chips are installed. BSA suggests the Committee urge the Department

---

[2] For additional information on BSA's recommendations for ICT supply chain security policies, see Building a More Effective Strategy for ICT Supply Chain Security, available at: US: Building a More Effective Strategy for ICT Supply Chain Security | BSA | The Software Alliance.

to exercise the authority already granted to it to develop an inspection regime under Section 224 of the FY19 NDAA. Under this authority the DoD could facilitate conformity testing of microcomponents, including PCBs, while continuing to enable procurement of commercial and COTS items.

### D. Implementing the Naval Sustainment System-Supply (NSS-Supply)

BSA is pleased that the Committee continues to support advancements in supply chain visibility. Improved visibility is critical to mapping supply chains, identifying vulnerabilities, and developing alternative and more secure sources of strategic goods and services. Increased visibility also promotes readiness and optimizes decision making by improving end-to-end logistics processes and data integration. Insights achieved through increased data integrity and expanded data analytics will drive necessary weapon system readiness improvements.

The United States Naval Supply Systems Command established a new end-to-end approach to managing naval supply chains and supporting mission performance. NSS-Supply seeks to implement a portfolio-based approach across the commercial and organic industrial base to increase predictability, capacity, and speed throughout the supply chain.

To support these ongoing improvements, BSA recommends the Committee direct the Secretary of the Navy to brief the Committee on the strategy to implement NSS-Supply, including explanations of the milestones and outcomes to be achieved under NSS-Supply; how the potential gains brought by NSS-Supply will be institutionalized to improve the end-to-end supply chain business process; and the resources needed to support NSS-Supply and a discussion of the potential to accelerate outcomes and the resources to do so.

## 2. Develop the Cybersecurity Maturity Model Certification (CMMC)

In November 2021, the DoD announced CMMC 2.0 with an updated program structure designed to achieve the DoD's cybersecurity goals. The DoD intends to implement this updated program structure through a regulatory process, to include a public comment period, over the next year or two. 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. Ensuring Clarity for Certification Requirements

Currently, the DoD has stated that if "contractors and subcontractors are handling the same type of FCI and CUI, then the same CMMC level will apply. In cases where the prime only flows down select information, a lower CMMC level may apply to the subcontractor."[3] It remains conceivable that a subcontractor may be required to attain one level of certification for one contract, only to find out that a higher level is required for a subsequent contract. The determination of the level of certification is based on the level of sensitivity of information being handled by a contractor on a per-contract-basis. The determination of level of sensitivity can vary from service to service or even contract to contract; in other words, if each acquisition authority is allowed to establish certification requirements on its own, two acquisition authorities may set different level requirements for substantially similar services. This approach could require contractors and subcontractors to undergo certification multiple times at different levels while providing similar services – a scenario that is costly and inefficient.

BSA recognizes the Department has taken steps to minimize re-certification through the use of its Supplier Risk Performance System (SPRS), which records a supplier's CMMC level of certification for contracting officer awareness. However, this assumes that the level of certification remains the same across various contracts. To help solve this problem, BSA recommends the Committee should require the Department to evaluate, based on previous contracting histories, the anticipated certification

---

[3] OUSD A&S - Cybersecurity Maturity Model Certification (CMMC) (osd.mil)

requirements for contractors and subcontractors and provide upfront notification of these determinations.

    **B. Harmonizing CMMC with Related Government 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 it 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.

**3.    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.

These actions create significant cybersecurity risks into the Department's software development lifecycle. BSA recommends the Committee direct the Department to develop and publish policies for the acquisition and use of FOSS. In developing these policies, the Committee should require the Secretary to ensure that any external software acquired or developed for the use by the Department by any vendor, integrator, consultant, research center, or other organization, including software from an open-source community, to go through the same security evaluation, acquisition, and maintenance and sustainment processes, including: legal license review and records retention for the authorized usage and any modification of the software; vulnerability and reputation assessments of the software and its developing organization's(s') supply chain and primary developer community; compliance with NIST security standards; availability and designation of how and where to receive software support, including submitting and verifying security concerns with a designated response process from the developer; 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 any 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.

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.

Additionally, BSA suggests the Committee should encourage the DoD to digitize the Department's organic industrial base (OIB) maintenance and repair production operation. Military departments own and operate industrial facilities that manufacture, maintain, repair, and overhaul military weapons and equipment (collectively referred to as the OIB). The Department's OIB ensures effective and timely responses to mobilizations, national defense contingency situations, and other emergency requirements. These industrial facilities serve important national security functions and could perform more efficiently and effectively by leveraging the benefits of intelligent and adaptable automation technologies. BSA encourages the Committee to instruct the Department to review maintenance and repair operations within the OIB and identify opportunities to modernize capabilities through digital technologies.

### C. Overseeing Implementation of Section 835 of the FY21 NDAA

Ensuring that software is developed and deployed in a secure manner is essential for security, efficiency, and effectiveness at the Department. High-profile attacks from both advanced persistent threat actors and criminals over the last year have highlighted the importance of this issue.

BSA supports Section 835 of the FY21 NDAA, which requires the Department to develop requirements for a secure software development lifecycle. The Committee should ensure that the Department provides guidance and resources to vendors on what practices are needed and should also encourage adoption of existing standards and established practices rather than the creation of new ones. BSA encourages the Committee to review both BSA's Framework for Secure Software[4] and the National Institute of Standards and Technology's recently published Secure Software Development Framework[5] (which cites to the BSA Framework for Secure Software) as available frameworks.

### D. Encouraging Broader Use of Security Orchestration Tools

Software services play a critical role in securing sensitive data and networks, and security orchestration technologies are often at the cutting edge in this regard. BSA supports the pilot program created in the FY21 NDAA (Section 1733) on cybersecurity capability metrics, which would include an assessment of security orchestration technologies. We believe broader use of security orchestration tools within the defense enterprise could pay enormous dividends in improving the accuracy and efficiency of incident response.

### E. Adopting Software Solutions that Modernize Operations

As the Department, along with other parts of the Federal Government, examine opportunities to transform and digitize their processes to allow for greater security, efficiency, cost effectiveness, and to improve operations, BSA urges the Committee to consider policies to promote the adoption of digital transformation tools.

Remote online notarization (RON) is an example of an innovative solution that allows trackable, traceable, and fraud-resistant notarial acts be performed electronically and is especially beneficial to

---

[4] *See* Updated: BSA Framework for Secure Software | BSA | The Software Alliance.

[5] *See* Secure Software Development Framework | CSRC (nist.gov).

individuals unable to easily travel to access notarial services, such as active-duty military stationed overseas. Last year BSA supported the inclusion of the Securing and Enhancing Commerce Using Remote and Electronic (SECURE) Notarization Act, which unanimously passed the House of Representatives as Title LXV of H.R. 4350 of the FY22 NDAA. This provision complements state notarial laws while permitting nationwide use of RON, with key consumer protections, including multi-factor authentication of the signer and the use of tamper-evident technology, along with certainty for the interstate recognition of RON. BSA urges the Committee to again incorporate this language.

The Department has also experienced poor user experience because of a lack of focus on designing services and solutions. The Committee should consider directing the Department to prioritize design principles that relate to servicemembers' needs when adopting solutions. Similarly, adopting and utilizing SaaS solutions to automate processes could improve the delivery of business services to servicemembers and their families, and BSA suggests the Committee consider business reforms that streamline services delivered to the military and military families globally.

BSA also supports the DoD's efforts to accelerate implementation of the requirements of the 21st Century Integrated Digital Experience Act (21st Century IDEA), as well as the committee's oversight in this implementation. 21st Century IDEA requires that all federal executive agencies, including the Department of Defense modernize their citizen-facing websites, as well as internal-facing intranets, digitize paper-based forms, and plan for the increased use of electronic signatures to conduct departmental business. The department has made some strides in these areas, as reported in their 21st Century IDEA Report to Congress for 2021, but more needs to be done to fully meet the letter and spirit of 21st Century IDEA, across all areas highlighted by the law. In the FY2021 conference report that accompanied the National Defense Authorization Act (NDAA), the House Armed Services Committee supported the DOD's implementation of these requirements, while noting the significant positive impact full implementation of this law would have on the department's mission delivery and internal and external customer experience. As a follow-on in FY22, the Committee included additional directive language, noting the importance of a modernized DoD Public Web Program to ensuring DoD websites are secure, accessible, and mobile friendly to all who use them, including active duty and civilian personnel, military families, and the broader defense community. In light of this direction, and the criticality of the issues to be addressed, BSA supports the Committee's continued active oversight of implementation of 21st Century IDEA, including encouraging DOD to accelerate modernization of its websites via the Defense Media Activity, digitization of paper forms, and quicker deployment of electronic signature technologies.

### F.  Modernizing Management Capabilities

Section 836 of the FY21 NDAA directed the Department to develop and integrate advanced digital data management and analytical capabilities. The Department's ADVANA platform has real potential to serve as a baseline capability for enterprise data management. COTS data management capabilities must be more fully incorporated, however, to recognize fully the benefits of such a capability. BSA urges the Committee to direct the Department to integrate COTS products, including commercial XaaS offerings, to the greatest extent practicable, and to develop and submit to the Congressional defense committees a plan for such incorporation. Additionally, we suggest the Committee direct the Department to include budget justification information pertaining to the costs associated with implementing the enterprise data management system beginning with the Department's FY2023 budget request.

### G.  Ensuring Appropriate Implementation of Existing Security Requirements

BSA understands that the Defense Information Systems Agency's (DISA's) IL-5 heightened level of cloud security adds ten additional controls to its IL-4 security level intended to protect the use of sensitive data stored or accessed by cloud applications. BSA is concerned that DISA is potentially misapplying the Cloud Computing Security Requirements Guidelines (CC SRG) by requiring IL-5 compliance of cloud-based providers of digital identity verification solutions that enable workforce users to authenticate identity to access to IL-5 applications, but which do not themselves handle or store sensitive data protected by IL-5. DISA inferring a higher security requirement than is required potentially misapplies the CC SRG and prevents DISA from accessing best of breed, platform neutral, digital identity solutions from the American companies. BSA suggests the Committee request a briefing or report from DISA and DoD CIO to explain

whether and why IL-5 applies to digital identity verification software that authenticates users to IL-5 applications but does not itself store or access any sensitive data, and how DISA and the DoD CIO are working with the private sector to ensure DoD has access to the most effective solutions.

### H. Expanding Security Information and Event Management Services to Sensitive CUI

As the Committee recognizes, COTS security information and event management (SIEM) is integral to effective network security. This capability provides a single security management system that offers full visibility into customer's – including the DoD's – networks, thus allowing a security operations center to respond to a threat in real time. As the DoD continues to transition to a software as a service model, security must remain a key consideration. To ensure the DoD has access to the most innovative and effective services, BSA urges the Committee to direct the Department to explore expanding SIEM for higher sensitivity CUI 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.

### I. Modernizing the DoD's Data Logging

With the ever-increasing cybersecurity threat to national security systems and defense networks, such as SolarWinds and Log4j, BSA is concerned that the Department lacks an enterprise-wide standardized format for data logging called for in August 2021 through OMB-21-31, which was issued pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity. However, the DoD has not yet achieved what OMB-21-31 called for. Accordingly, BSA urges the Committee to direct the Department to submit to the Committee a report on its implementation plan for OMB-21-31, including plans for the use of COTS solutions, and to include associated funding for implementation with the Department's budget submission for FY2024.

### J. Implementing the Joint Transportation Management System

The United States Transportation Command has sought to implement the Joint Transportation Management System since 2016. This system seeks to bring efficiency to CONUS and OCONUS sustainment and freight transportation efforts for the military services, DoD agencies, and the National Guard. Since the system was identified as the preferred solution, the DoD has executed several pilot programs, which have demonstrated promising results. However, it is unclear how the Department plans to implement this program. BSA recommends the Committee direct the Department to brief the Committee on its strategy, timeline, and resource requirements to implement the Joint Transportation Management System.

## 4. 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) and PaaS have proven to be more effective and efficient. 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 innovation 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. Improving FedRAMP

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. The problems are exacerbated by the limited reuse of authorizations to operate (ATOs).

Numerous proposals and programs both inside and outside the DoD have led to a disjointed approach to cybersecurity across the US Government. Multiple silos of cybersecurity standards and requirements have evolved at different agencies hindering a unified approach to cybersecurity at all levels of data classification.

BSA therefore recommends that the Committee direct the Comptroller General to submit a report to the Armed Services Committees on the laws and regulations impacting the US Government's approach to procurement. The report should describe how 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 program 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 coordinating among different certifications and authorizations to meet the Federal Government's modernization and security objectives.

### B. Migrating the DoD to Commercial Cloud Services

DISA is tasked with the migration of DoD applications and services from DoD-owned data centers to commercial cloud services. DISA must provide guidance for this migration to work, including the basis on which DoD can assess the security of both DoD-owned and commercial cloud services. For this transition to be successful, the process DISA uses must be clear and transparent.

BSA understands that DISA's IL-5 heightened level of cloud security adds ten additional controls to its IL-4 security level intended to protect the use of sensitive data stored or accessed by cloud applications. BSA is concerned that DISA is potentially misapplying the CC SRG by an overzealous requirement for IL-5 compliance of cloud-based providers of digital identity verification solutions that enable workforce users to authenticate identity to access to IL-5 applications, but which do not themselves handle or store sensitive data protected by IL-5. DISA staff inferring a higher security requirement than is required potentially misapplies the CC SRG preventing DISA access to best of breed, platform neutral digital identity solutions from the American tech sector. BSA suggests the Committee request a briefing or report from DISA and DoD/CIO explaining whether IL5 applies to digital identity verification software that authenticates users to IL5 applications but does not store or access any sensitive data itself, and what DISA and DoD/CIO are doing to work with the private sector to remediate.

BSA recommends that the Committee instruct DISA to provide the Committee regular reports detailing the process for accrediting cloud service providers, how that process is being communicated to potential vendors, and the status of applications for accreditation as well as submit a report clarifying whether and under what authority DISA waives CC SRG compliance thresholds to require IL-5 controls on commercial cloud applications that do not otherwise trigger the requirement.

### C. Leveraging Multi-Cloud Solutions

Given the benefits of multi-cloud solutions which have previously been recognized by the House Appropriations Committee in the DoD's FY 2020 Appropriation,[6] BSA suggests the Committee direct the FAR Council to advise agencies procuring enterprise cloud services for IaaS or PaaS (as those terms are defined in NIST 800-145) that, for the sake of consistency and predictability in government planning and access to cutting-edge products and services at competitive prices, cloud requirements shall be set forth consistent with the statutory general preference (*e.g.*, 10 USC 2304a) for contract awards to multiple vendors under a task and delivery order contract or a single award to a cloud integrator with multiple cloud service providers as vendors. Where specific mission requirements require an agency to deviate from utilizing a multivendor IaaS or PaaS cloud environment, that agency may do so provided that, prior to procuring the subject cloud services, the Agency Head determines in writing that agency mission requirements necessitate deviating from the preference for multiple IaaS and PaaS contracts. Agencies shall report all such deviations issued in the fiscal year to the appropriate House and Senate committees.

Further, some cloud service models incentivize migrating data to the cloud by offsetting or waiting data egress fees (charges a cloud service provider bills to customers to defray the cost of moving their data from one CSP to another CSP or the customer's own data center), that in many cases would otherwise make it cost prohibitive to move one's data from one provider to another. Egress fees can make it cost-prohibitive to switch CSPs or work with more than one, as is considered best practice. BSA is concerned that DoD has not accounted for these costs, and that they create lock-in effects and barriers to multi-cloud use. <u>BSA urges the Committee to direct the Comptroller General of the United States to submit a report to the appropriate Congressional committees on the impact of data egress fees on the DoD's transition to cloud services</u>, including: if data egress fees result in vendor lock-in, and the costs associated with any potential lock-in; how egress fees and related adjustments limit multi-cloud and hybrid cloud architectures, or other requirements; how the Department is addressing the risks associated with data egress fees; if the Department's risk mitigation plan is sufficient; if the department would benefit by requiring that future cloud service procurements prohibit or limit data egress fees; what, if any, egress fees should be allowable; and any additional matters the Comptroller General determines appropriate.

## 5. Fund Research and Development

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 identifies the below opportunities as particularly valuable for the Committee to support.

### A. Prioritizing AI Research Investments to Enhance Operational Effectiveness

U.S. national security is increasingly dependent on the DoD's ability to leverage and integrate AI into its systems. In March 2021, the Congressionally mandated National Security Commission on Artificial Intelligence (NSCAI) issued its final report to the White House and Congress with a list of ten Priority Areas for AI Research Investment, which included: Integrated AI modeling, simulation, and design; Enhanced human-AI interaction and teaming; and Advanced Scene understanding.

<u>BSA recommends that the Committee prioritize funding for AI research that advance these priority areas, including several ongoing programs within DoD</u>, specifically:

- The Air Force Joint Simulation Environment (JSE), which is part of the initial operational test and evaluation component of the F-35 program.
- The Army Synthetic Training Environment (CSTE), which will allow soldiers to conduct realistic training anywhere in the world and enable interoperability with future operational capabilities.

---

[6] The House Appropriations Committee, in its report accompanying DoD's FY 2020 Appropriation, recognized that, as DoD was pursuing a single cloud solution, other agencies were taking a multi-cloud approach based on value to themselves and their programs. U.S. House of Reps., Rept. No. 84, 116th Cong., 1st Sess., 2019 at 12.

- The Air Force Research Lab Information Directorate's "Fight Tonight" program would augment human decision-making through a combination of AI and gaming technologies.

### B. Supporting Appropriations for AI and Quantum Computing Research

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 encourage 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.

### C. Supporting R&D in Technologies that Can Foster Supply Chain Security

BSA appreciates the Committee's support for standardizing supply chain security best practices to improve its acquisition of securely manufactured commercially available products. There is also an opportunity for the Department to lead in the supply chain security arena by investing in the R&D of new technological approaches to fostering supply chain integrity. Promising areas of research include the use of blockchain-based technologies, development of processes to vet third-party components for security issues, and the application of AI for the analysis of supply chain data and anomaly detection, among others. BSA suggests the Committee ensure that the FY23 NDAA dedicate funding specifically for R&D into supply chain technologies through partnerships with academic institutions and other technology leaders.

### D. Investing in Technology Solutions to 5G Security Challenges

Over the long run, the most successful strategy for addressing challenges to 5G supply chain security and cybersecurity will be to invest in innovation. Technologies such as standards-based, virtualized radio access network solutions supporting open interfaces, for example, hold the potential to transform the marketplace in ways that foster a more diverse, competitive supplier base that can compete on the grounds of security. Cultivating secure, open architectures will be important foundations for these technologies and will enable further innovation. In addition, as 5G dramatically expands the volume of data transiting networks, new approaches to encryption will be vital. BSA supports Section 225 and 9202 of the FY21 NDAA, which establishes an Innovation Fund for 5G. Among other things, the Innovation Fund is designed to support the development of open standard-based and interoperable solutions, and open architectures. This can help ensure that the Department not only has many suppliers to choose from but is prepared to operate securely in this rapidly evolving environment.

## 6. Provide Resources for Capacity Building and US Leadership

As the Department and the broader US Government increasingly confront challenges that are innately transnational – such as securing complex supply chains, combatting malicious cyber actors, and maintaining resilience for global operations – BSA believes international cooperation is more important than ever.

Currently, the US Government's capacity-building tools for cybersecurity are under-resourced. BSA supports the establishment of dedicated US government cybersecurity capacity-building tools through the Departments of State, Defense, and Commerce, and we urge the Committee to evaluate existing capacity-building authorities to determine whether they are sufficient to fully support global cybersecurity capacity-building initiatives.

The Department should also continue to lead on ethical practices and policies. BSA firmly believes that AI can do great things, but we recognize that it must be developed and deployed responsibly. In the FY21 NDAA, the Committee directed the Department to consider acquisition of AI that is ethically and responsibly developed. This was an important step and BSA supports continuing to ensure these values

drive the DoD's AI acquisitions as well as encouraging other countries to adopt the same or harmonized standards.

## 7.  Build a Workforce for the Present and the Future

As BSA recognized when, in October 2021, it released Strengthening Trust, Safeguarding Digital Transformation: BSA's Cybersecurity Agenda, "building a secure future is not possible without developing an effective cybersecurity workforce." As our digital transformation continues, expedited by the COVID-19 pandemic, 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.

The Committee can help build the workforce of the present and the future by:

### A.  Increasing Investments in STEM and Computer Science Education

As the March 2021 final report of the Congressionally created NSCAI recommended, BSA supports Congress passing a second National Defense Education Act, focusing on funding for students to learn digital skills, including mathematics, computer science, information science, data science, and statistics, across the education system, including in K-12 schools, community colleges, and university, and through reskilling programs.[7] The investments directed by the bill should target disciplines that lead to skills valuable in the fields of AI, quantum computing, and cybersecurity.

### B.  Developing Technology Talent of DoD Personnel

The DoD, like every employer, increasingly needs personnel with digital skills and knowledge to effectively carry out its mission. The Department, however, faces unique challenges in retaining, recruiting, and developing personnel. BSA supports further investment in training and reskilling DoD personnel as well as expanding ways the DoD can build its future workforce.

### C.  Educating the Acquisition Workforce

As technology generally, and software specifically, become increasingly integral to the DoD's ability to accomplish its mission, it is becoming more important that the personnel tasked with acquiring these tools have the necessary knowledge and skills, to deliver for the Department and its stakeholders. BSA strongly supports the Committee's efforts to support DoD efforts to attract, educate, retrain, promote, and retain tech talent.

<div align="center">

\#      \#      \#      \#

</div>

We would welcome the opportunity to work with you and your staff to address these ideas in the FY23 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*

Victoria A. Espinel
President and CEO

---

[7] National Security Commission for Artificial Intelligence (NSCAI), Final Report (Mar. 1, 2021), at 173, available at Full-Report-Digital-1.pdf (nscai.gov).