



March 26, 2020

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

Dear Chairman Inhofe and Ranking Member Reed:

As you prepare to develop the *Fiscal Year 2021 National Defense Authorization Act* (FY21 NDAA), we write to you to offer the perspective of the software industry on key legislative efforts we believe could improve our national security and enhance the ability of the Department of Defense (DoD) to innovate.

BSA | The Software Alliance (BSA)<sup>1</sup> is the leading trade association representing the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, developing cutting-edge solutions in use across the range of information technology (IT) platforms, and are global leaders in advancing best practices for developing quality, secure, trustworthy software. As such, our members share the interests of the DoD and the Armed Services Committee in ensuring the highest standards of cybersecurity, driving agile and meaningful innovation, and harnessing emerging technologies.

Both as the Federal Government's largest department and as the government's leading innovator of security technologies, DoD is well positioned to play a leading role in setting policy courses in relation to software development, cybersecurity, and workforce development that can serve as examples to the rest of the government and beyond. We are therefore eager to work with you to ensure that Congress and the Department leverage this leadership opportunity and craft policies that advance security,

---

<sup>1</sup> BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, IBM, Informatica, Intel, Microsoft, Okta, Oracle, PTC, salesforce.com, ServiceNow, Siemens PLM Software, Sitecore, Slack, Splunk, Trimble Solutions Corporation, The MathWorks, Trend Micro, Twilio, and Workday.

innovation, and competitiveness simultaneously. To that end, we wish to share with you our priorities for the FY21 NDAA.

### ***Cybersecurity Maturity Model Certification***

The Department has been working to develop a new framework – the Cybersecurity Maturity Model Certification (CMMC) – to build assurance around information security practices of Defense Industrial Base contractors and subcontractors. As an association representing industry leaders in information security and supply chain risk management, BSA commends the Department’s initiative and shares its goals. In order to ensure the success of the CMMC initiative, we believe that current proposals for implementing the CMMC can be improved with regard to clarity and predictability about its scope and processes. Addressing these areas can help the DoD avoid unnecessary confusion and delay in the CMMC’s implementation.

To ensure that the CMMC realizes its goals, the Committee should provide clear guidance to the Department to clarify key questions. Specifically, the Committee should:

- *Ensure predictability for certification requirements.* The current proposal asserts that certification requirements for DIB subcontractors will flow down from prime contractors in relation specifically to the contracts on which they are working. It is conceivable – potentially even likely – 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. Such risk could be exacerbated if no centralized approach to determining certification requirements is established; 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, based on changing contract requirements – a scenario that is costly and inefficient. Instead the Committee should require the Department to evaluate, based on previous contracting histories, the anticipated certification requirements for contractors and subcontractors and provide upfront notification of these determinations.
- *Clarify the scope of coverage.* The CMMC Model and accompanying materials provide only limited information about the intended scope of certification requirements, leaving several important questions unanswered. For example, it is also unclear whether certification would be required in cases in which a subcontractor handles no controlled unclassified information or is a non-US company. It also remains uncertain whether the certification requirements will apply to COTS vendors in general and whether they will apply to non-procurement contracts such as cooperative agreements and grants. The Committee should establish a clear mandate for the CMMC that clarifies the scope of its coverage.
- *Synchronize with related government efforts.* DoD should align the CMMC with other Defense Department and federal cybersecurity and supply chain security requirements (such as the DoD Cloud Computing Security Requirements Guide, DFARS 252.204-7012, and FedRAMP) to the greatest extent possible to avoid or eliminate duplication. Particularly, DoD should look to leverage FedRAMP for CMMC designations at the product level when the contractor is using a cloud for its CMMC solution (i.e. for servers, hardware, IaaS, PaaS, and SaaS). While CMMC covers a broader range of products and services, those companies that have FedRAMP and SRG authorizations already surpass the vast majority if not all of the CMMC’s control requirements, certainly at CMMC Levels 1-3, since FedRAMP requires continuous monitoring and improvement. Allowing for reciprocity with other cybersecurity requirements will reduce cost and administrative burden and allow DoD to achieve its cybersecurity goals on a quicker timeline. The

Committee should require DoD to identify and establish reciprocal recognition of other available certifications that meet CMMC goals.

### ***Supply Chain Security***

As the Department of Defense and the broader Federal Government continue to wrestle with how to best secure supply chains against malicious threats and inadvertent risks, BSA urges the Committee to exercise its leadership in working to craft policy solutions that can effectively advance supply chain security without disrupting innovation and global digital commerce. Doing so requires a careful, transparent, multi-stakeholder process to understand the impact of potential courses of action across the broad array of actors impacted by supply chain interventions.

BSA expects the Committee to consider proposals for addressing supply chain risks in addition to CMMC, and urges the Committee to evaluate such proposals against the following principles:

- Supply chain policies should embrace internationally recognized, industry driven standards for security throughout the digital supply chain.
- Supply chain policies should be rooted in risk management approaches that prioritize security measures based on the most relevant and potentially impactful risks.
- Supply chain policies should be transparent to the public, with specific actions notified to impacted stakeholders, and should establish meaningful mechanisms for resolving disputes.
- Supply chain policies should be enforceable, for example by establishing supply chain risk management responsibilities in vendor contracts.
- Supply chain policies should be collaborative, embracing public-private partnership, information-sharing, and operational cooperation.

In addition, BSA urges the committee to establish as US policy that the Department will refrain from systemic interventions in global supply chains. Enhancing supply chain security means, in part, developing a more secure global cybersecurity ecosystem that recognizes norms for responsible behavior and prioritizes collective defense against malicious threats. The Congress can send an important message by stating that it is the policy of the United States that the Department will not undertake systemic interventions in global supply chains in connection with its Title 10 defense responsibilities.

Finally, we urge the Committee to maintain rigorous oversight of the DoD's implementation of key provisions of previous NDAs relating to supply chain security, including Sections 889, 1654, and 1655 of the Fiscal Year 2019 NDAA. BSA supports Congress's efforts to ensure the security and integrity of the US Government's supply chains, but believes continued oversight of the implementation of these provisions is important to prevent unintentional consequences for responsible developers and customers of technology solutions. BSA looks forward to working with the Committee to ensure that the Department's implementation is transparent, that it solicits and incorporates feedback from impacted stakeholders, and that it advances models for software assurance that operate effectively in a global context.

### ***Software Acquisition and Security.***

BSA applauds the Committee for passing meaningful legislation in last year's NDAA to reform the Department's software acquisition practices, based on recommendations from Defense Science Board and Defense Innovation Board studies. We are eager to see the Department continue work to implement these measures. In addition, we believe additional steps would improve the Department's ability to access the most innovative, secure software available:

- *Embrace 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, the Committee should establish a clear, mandatory preference for best-in-class COTS software where such software can meet the Department's requirements.
- *Ensure that security is integrated throughout the software acquisition lifecycle.* Building secure software is paramount to the Department's overall cybersecurity posture. A recent Government Accountability Office (GAO) study found "mission-critical cyber vulnerabilities in nearly all weapon systems that were under development." To prevent such vulnerabilities in the future, the Department must begin to integrate security considerations throughout the software acquisition lifecycle, from program design to end-of-life. To that end, the Committee should consider requiring all software development or acquisition programs to articulate a secure development lifecycle during contract competition or program inception; likewise, the Committee should consider requiring the development of security metrics, such as defect density, to assess performance of software acquisition programs.

### ***Research and Development***

BSA appreciates the Committee's commitment to supporting research and development (R&D) efforts at the Department, particularly basic and applied research into emerging technologies such as artificial intelligence (AI) and quantum computing. Specifically, BSA urges the Committee to:

- Support funding for quantum computing research and artificial intelligence without cutting basic R&D. BSA strongly supports robust investments in quantum computing and artificial intelligence at the Department, and appreciates the Administration's proposed budget increases in these areas. Yet, 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. We strongly support proposed 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.
- Support research and development into technologies that can foster supply chain integrity. 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 research and development 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 artificial

intelligence for the analysis of supply chain data and anomaly detection, among others. The FY21 NDAA should dedicate funding specifically for research and development into supply chain technologies through partnerships with academic institutions and other technology leaders.

- Invest in technology solutions to 5G security challenges. BSA believes that, 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 virtualized radio access network solutions, 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. Secure, open source-driven architectures will be important foundations for these technologies, and will enable further innovation. In addition, as 5G dramatically expands the volume of data transiting communications networks, new approaches to encryption will be vital. Investing R&D funds to support the acceleration of research in these areas, and to incentivize the development of open standards and open source-driven architectures, can help ensure that the Department is prepared to operate securely in this rapidly evolving environment.

### **Capacity Building**

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. For that reason, in our newly released cybersecurity policy agenda, *Securing Tomorrow: BSA's Cybersecurity Priorities and Software's Essential Role*, BSA advocates for expanding efforts to build international capacity for good cybersecurity governance. The Department can improve the ability of foreign partners to contribute to tackling transnational challenges by investing in building their cybersecurity capacity. Currently, U.S. government capacity-building tools for cybersecurity are underdeveloped. BSA supports the establishment of dedicated U.S. government cybersecurity capacity-building tools through both the State and Defense Departments, 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.

### **Cyberspace Solarium Commission**

BSA welcomes the report from the Cyberspace Solarium Commission, and commends the Committee for supporting that Committee's establishment. The report's recommendations of new strategies to secure the United States against an increasingly diverse and sophisticated series of cybersecurity threats represent a compelling and much-needed roadmap toward bipartisan solutions to longstanding challenges. While some of the Commission's recommendations may demand more in-depth consideration or may fall outside of BSA's areas of focus, we strongly support many of its proposals and urge the Committee to consider relevant legislative proposals to the greatest extent possible. Specifically, BSA supports the Commission's recommendations to:

- **Strengthen the U.S. Government's structure**, including by establishing a National Cyber Director and strengthening the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security.
- **Diversify and strengthen the cybersecurity workforce** by improving the federal cyberspace workforce and enhancing cyber-oriented education at all levels.

- **Strengthen norms and non-military instruments of power** by creating a Cyber Bureau and Assistant Secretary at the U.S. Department of State, improving international cybersecurity capacity-building activities, working to strengthen international norms, and enhancing engagement in international standards development.

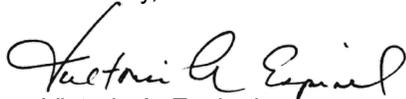
Two other sets of recommendations included in the Commission's report stand out as particularly of interest to BSA's members. First, the report proposes a National Cybersecurity Certification and Labeling Authority empowered to manage a program for voluntary security certifications and labeling. Certifications and labels can be highly effective tools for promoting trust and communicating critical security information between customers and vendors. Our members' products and services hold security certifications and labels from authorities around the world. In our experience, such regimes are both most effective and most conducive to efficient business operations when they are tied to well-established, internationally recognized standards. As certification regimes proliferate globally, it is essential that new schemes in the United States are harmonized with existing efforts to the greatest extent possible. This is particularly true for the report's proposed cloud security certification, in light of the numerous existing and developing cloud certification efforts around the world.

Second, in addressing cloud services, the report also calls for incentivizing broader cloud adoption for small and medium-sized organizations. As leading providers of cloud services, our members strongly agree with the Commission about the potential operational and security benefits cloud platforms can bring to small and medium-sized organizations. The Department of Defense can play a critical role in incentivizing broader cloud adoption, particularly given its deep relationships with thousands of small and medium-sized businesses across the United States.

We would welcome the opportunity to work with you and your staff to address these ideas in the FY21 NDAA. Working together, we can forge a deeper partnership between Congress, DoD, and the technology sector to advance national security and foster transformative innovation.

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

Sincerely,



Victoria A. Espinel  
President and CEO