Ms. Linda Neilson
Director
Defense Acquisition Regulations System
United States Department of Defense

RE: Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)

BSA | The Software Alliance (BSA)[1] is grateful for the opportunity to provide comments to the Department of Defense (DoD) on its interim Defense Federal Acquisition Regulation Supplement (DFARS) rule implementing the Cybersecurity Maturity Model Certification (CMMC) program.

BSA 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 cybersecurity. As such, its members supply the Department of Defense with software, cloud services, cybersecurity systems, and other information technologies that are critical to advancing the Department's mission and defending its networks against adversaries.

I. Introduction

Because of the range of products and services they provide to the Department, including custom-built, commercial item, and commercial-off-the-shelf (COTS) products and services (including cloud services), BSA's members have a particular interest in the implementation of the CMMC program, which establishes a maturity model setting forth tiers of cybersecurity requirements against which DoD vendors are to be certified.

BSA's members are strongly supportive of the CMMC's goal to improve protection of controlled unclassified information in the DoD supply chain. Inadequate security of controlled unclassified information can endanger U.S. national security, undermine DoD acquisitions, and put the intellectual property and trade secrets of DoD suppliers at risk. To that end, BSA and its members have provided feedback to the Department throughout the development of the CMMC framework and have also contributed to other key supply chain risk management efforts such as NIST Special Publication 800-171 and the Open Group's Open Trusted Technology Provider Standard (O-TTPS).

Despite these shared goals, BSA has significant concerns about the approach embodied in the Interim Rule. It would create a bureaucratic approach that is so cumbersome, costly, and lacking in clarity that it may be impossible to implement. BSA wonders whether DoD could make better use of the many existing approaches to supply chain risk management currently in operation, combined with more robust security guidance to and vetting of members and broader adoption of automated cybersecurity technologies, in order to achieve a less costly, more practical solution to this challenge.

[1] 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.

As the Department considers a final rule and moves forward in implementing CMMC requirements, BSA notes four significant concerns: (1) reciprocity with other information security initiatives, (2)) the rules, guidelines and procedures that govern the requirement for DoD contractors to assess their security based on NIST SP 800-171, (3) the scope of coverage, (4) communication of CMMC requirements to contractors and subcontractors, and (5) the Department's approach to certification. We offer specific suggestions for remediating these concerns. Each of these concerns is examined in greater detail below. Nevertheless, even if these concerns were to be remediated, BSA fears that the enormous scope of the program and its cumbersome bureaucratic burden will prevent the CMMC from being an effective approach to enhancing information security, much less one that guards against excessive costs to industry participants and taxpayers.

II. Reciprocity

A leading concern about CMMC implementation is whether it will duplicate existing efforts to secure sensitive information in the supply chain. Depending on the type of product or service, DoD vendors may already be subject to assessment, certification, or direction under a number of existing initiatives across DOD and the Federal Government. For example, DoD vendors of cloud services may already be subject to DoD's Cloud Computing Security Requirements Guide (SRG), the Federal Risk Authorization and Management Program (FedRAMP), security requirements embedded in individual contracts, and audit processes such as those from the Defense Contract Management Agency. Moreover, many vendors may obtain certifications against internationally recognized standards that attest to security controls covered by the CMMC. It is unclear how CMMC certification, above and beyond these existing obligations, would improve the Department's confidence in the security practices of such vendors.

Nevertheless, the Department has left significant ambiguity regarding whether certifications under such existing initiatives would be reciprocally recognized under CMMC. Despite public statements by the Department providing assurance that CMMC certification would include reciprocity, the question is not addressed in the Interim Rule, and the Department has not published any specific guidance addressing reciprocity. In fact, the interim rule further complicates matters because DFARS 252.204-7020 requires assessments conducted by the Defense Contract Management Agency (DCMA), implemented through a DCMA-developed methodology, on top of CMMC requirements.

Absent reciprocity, the CMMC would unnecessarily increase the compliance burden on industry suppliers that have already demonstrated effective controls for protecting sensitive information. This outcome would increase costs for industry and for the Department. BSA urges DoD to align the CMMC with existing federal cybersecurity requirements to the greatest extent possible to avoid redundancy and prevent businesses from facing exorbitant costs stemming from having to maintain multiple, overlapping audits.

III. NIST SP 800-171 Assessment Requirements

Though CMMC is implemented over the next 5 years, the Interim Rule requires contractors (and their subcontractors) to immediately post an assessment of their cybersecurity compliance ("Assessment"), based on NIST SP 800-171, on the DoD's Supplier Performance Risk System (SPRS). This requirement is intended to allow the DoD to verify that a prospective vendor has a current (less than 3 years old) Assessment on record prior to awarding a contract. While many contractors may already be subject to this requirement under existing contracts, posting the required Assessment may pose a significant administrative and financial burden for contractors that have not recently assessed their level of

compliance and will need to commit the time and resources to obtaining a new Assessment. We recommend extending the deadline by which information must be reported into SPRS, and when contracts will be awarded based on these Assessments, by at least one-hundred and eighty (180) days, until March 1, 2021. This will provide companies that do not have a current Assessment several months to be able to plan and execute an Assessment for SPRS, and also allows for the fact that many DoD contractors have already spent significant time and resources trying to prepare for CMMC assessments, despite the lack of adequate guidance and a clear path forward for CMMC.

Similarly, the Interim Rule specifies three Assessment levels: Basic, Medium and High, with a Basic Assessment being a self-assessment completed by the contractor, while Medium or High Assessments are completed by the DoD (e.g. the Defense Contract Management Agency (DCMA)). Under the Interim Rule, Basic Assessments will result in a confidence level of "Low" because it is a self-generated score. While the Interim Rule states that procurements will require a certain Assessment level, it does not provide details on the processes and procedures for determining appropriate levels, or the competitive implications of an Assessment rating or confidence level during the source selection process. Further, DoD has provided no assurance that DCMA will have sufficient resources to conduct Medium or High Assessments in a timely fashion for all industry participants who seek them.

Furthermore, given the short window of time allotted to submit Assessments, contractors could face heightened risk of liability for a self-assessment that is not conducted or reported correctly. Contractors could also become liable for the attestations and Assessments of their subcontractors. As a result, we recommend that contractors be given notice of any deficiencies in an Assessment and the ability to challenge or remediate issues identified in DoD Assessments. We also recommend that a safe harbor rule be implemented to shield contractors from liability when Assessments are conducted and attestations are made in good faith. Furthermore, contractors should be shielded from liability stemming from their subcontractors when those subcontractors have acted in good faith.

Lastly, we recommend that safeguards and appropriate rules be put in place that would tend to prevent the Interim Rule from increasing the likelihood of bid protests stemming from reported Assessments. For example, for Medium or High level government Assessments, one contractor being able to schedule a DCMA Assessment sooner may result in an unfair competitive advantage.

In light of the above issues, we recommend that the provisions within the Interim Rule calling for contractors to assess and report their compliance with NIST SP 800-171 be reexamined and adjusted to address the above issues, and that the November 30, 2020 deadline for reporting Assessments be extended, at minimum, for an additional one-hundred and eighty (180) days, to March 1, 2021.

IV. Scope.

The Interim Rule intends CMMC requirements "for use in all solicitations and contracts or task orders or delivery orders, excluding those exclusively for the acquisition of COTS items." BSA appreciates that DoD has clarified that CMMC will not apply to strictly COTS items, the rule leaves a number of unanswered questions about its application. For example, will CMMC requirements apply to COTS items with custom installations or configurations, or slight modifications customizing them for the Department? Will CMMC requirements apply to subcontractors that supply COTS components for custom-built DoD items? Will CMMC requirements apply to non-traditional agreements such as cooperative agreements, Other Transaction Agreements (OTAs), and grants?

In any final rule, the Department should clarify the scope of the rule's application, addressing its coverage of the many diverse types of acquisitions in which the Department routinely engages.

V. Communication of Requirements to Contractors and Subcontractors

As the model is currently structured, requirements for a CMMC certification at a certain level are tied to individual contracts, and certifications are required to be current at the time of the award of an individual contract. Therefore, the only guidance the Department anticipates providing to its contractors and subcontractors on the level of CMMC certification they may, as an organization, require will come through individual contracts. Yet, DoD contractors and subcontractors generally compete for multiple contracts annually, creating the potential for confusion or duplication of effort. For example, it is conceivable that a contractor may compete for a contract requiring one level of certification, obtain that certification, and then subsequently learn that a higher level of certification is required for a separate contract. Absent any guidance, contractors may be forced to obtain multiple certifications in response to different contracts, or to invest in a higher level of certification than is needed to prepare for the uncertainty of future contracts. Because of the substantial costs of obtaining higher-level certifications, as detailed in the Federal Register Notice accompanying the Interim Rule, such confusion or redundancy can have significant financial consequences for defense suppliers.

Adding to this uncertainty is the Interim Rule's silence on how contracts will be selected for CMMC application, and how contracts, once selected, will be assigned a CMMC certification level. Absent clarity on how evaluation requirements will be determined, contractors have little ability to predict and plan for forthcoming certification needs.

The Department of Defense maintains data on the estimated 220,000 contractors and subcontractors with which it works. BSA recommends that the Department draw upon this data, including data about contractors' and subcontractors' previous work for the Department, to provide these contractors and subcontractors with initial guidance on the level of certification each one is likely to require. Such up-front guidance would avoid confusion and duplication, preventing unnecessary costs to industry and the Department. In addition, the Department should publish guidance on how contracts will be selected for CMMC, and how certification level requirements will be assigned to selected contracts. Such guidance should also help program managers and contracting officers understand how to segregate Statements of Work into separate sections with different CMMC levels, where appropriate, and provide instructions to prime contractors on how to flow down requirements within those separate sections to their subcontractors.

VI. Certification Methodology

While BSA understands that the Department of Defense seeks to create private sector-based certification infrastructure in order to enable it to meet the requirement for certifications across such a large group of vendors, the current approach creates a number of challenges undermining the integrity of the process, including potential for conflicts of interest, profiteering, and outsourcing of an inherently governmental function. The establishment of an independent Accreditation Board composed of representatives from the Defense Industrial Base holds the potential to put industry representatives in a position to oversee evaluation of their competitors, a troubling potential conflict.

Moreover, by outsourcing the oversight function to the private sector, it creates risk that individuals could take advantage of the Board's responsibilities to seek inappropriate profit. This risk unfortunately

was illuminated in practice recently when it was revealed that the Board's leadership had developed a scheme to name Accreditation Board "Partners" based on payments of up to $500,000. Such risks are exacerbated by lack of clarity about how certification fees will be maintained. The Federal Register Notice notes that costs for certifications "will be driven by multiple factors including market forces;" however, it does not provide any information regarding whether the Department or the Accreditation Board will be responsible for monitoring or controlling these costs.

To avoid potential conflicts of interest and the possibility of outsourcing inherently governmental functions, DoD must substantially re-work its approach to certifications. One approach would be for the Department to re-establish the Accreditation Board as a government body, and to put in place guiderails to prevent excessive certification pricing or other abuses. In any event, the current approach must be revisited.

VII. Conclusion

BSA strongly supports the Department's goal of enhancing the security of its supply chain and the sensitive unclassified information within it. Doing so will require effective collaboration between the Department and the technology industry and, indeed, BSA's members already work closely with the Department to strengthen its cyber defenses. The CMMC and accompanying interim Assessment requirements, while well intentioned, could undermine such collaboration and impose substantial administrative and financial burdens on both industry and the Department, all without a high degree of confidence that it would substantially improve information security beyond existing initiatives. BSA encourages the Department to reconsider this approach, including by revisiting assumptions about the need for such a broad approach to address products and services, such as cloud computing services, where robust security initiatives already exist.

BSA and its members stand ready to work with the Department to develop practical, implementable solutions that can enhance information security across the supply chain. We appreciate your consideration of our feedback, and look forward to more detailed discussions as these policies evolve.

Thank you for the opportunity to comment on this important matter.

Sincerely,

Tommy Ross
Senior Director, Policy