October 15, 2024

Via Electronic Submission

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

The Alliance for Digital Innovation (ADI) appreciates the opportunity to submit comments to the Department of Defense regarding our concerns with the proposed rule *Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements* (DFARS Case 2019-D041).[1]

ADI is a non-partisan alliance that advocates for the removal of institutional and bureaucratic barriers to the operation of a modern digital government. Our members provide key critical technologies to the federal government, including cloud infrastructure, digital identity solutions, human resources software, quantum computing, digital services, and a range of sophisticated cybersecurity tools and services. We support the adoption of innovative commercial technologies by the Federal Government.

ADI recognizes the need to appropriately secure Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) via the *Cybersecurity Maturity Model Certification* (CMMC) Program. In February 2024, we submitted comments[2] to the Department of Defense (DoD) regarding our concerns with its proposed rule for new requirements for CMMC 2.0.[3] We hope that our comments on this rulemaking - which focus on six key issue areas - will lead to a successful implementation of the new CMMC 2.0 requirements for federal contractors.

1. Regulatory Compliance Burden

ADI members are concerned about the increased regulatory compliance burden that federal defense contractors and subcontractors will experience under the CMMC 2.0 program. Specifically, while CMMC 2.0 has streamlined the five certification levels of CMMC 1.0 down to only three levels, it still requires the implementation of numerous advanced cybersecurity practices for contractors to achieve Level 3 (Expert). Moreover, CMMC 2.0 expands the number of security domains covered from the original

[1] https://www.federalregister.gov/documents/2024/08/15/2024-18110/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of

[2] https://alliance4digitalinnovation.org/wp-content/uploads/2024/02/02.26.2024-ADI-final-comments-on-CMMC-Proposed-Rule.pdf

[3] https://www.federalregister.gov/documents/2023/12/26/2023-27280/cybersecurity-maturity-model-certification-cmmc-program

CMMC 1.0 model. Although these changes help provide DoD with a more comprehensive view of contractor and subcontractor operations, they also dramatically increase the compliance burdens. Here, ADI members are concerned that contractors and subcontractors may decide it is no longer cost effective to do business with the DoD, especially if they are small and medium-sized enterprises (SMEs) or are required to reach Level 3. If this occurs, the DoD will have a less competitive marketplace in which the solutions become more expensive.

2. Reciprocity & Harmonization

Wherever possible, the DoD should make the DFARS CMMC 2.0 rule reciprocal with other information technology (IT) security frameworks that use the same underlying controls. Specifically, DoD harmonize its reciprocity process[4] with the General Services Administration's (GSA) Federal Risk and Authorization Management Program (FedRAMP) and the DoD's Cloud Computing Security Requirements Guide (SRG) security frameworks, since they also draw from controls in the National Institute for Standards and Technology's (NIST) *Special Publication (SP) 800-53 Security and Privacy Controls for Federal Information Systems and Organizations* Revision 5.[5] As the FedRAMP program management office updates its guidance, the CMMC team and DoD Chief Information Officer should review and update its guidance to reflect any changes to increase reciprocity. Where it does not establish reciprocity, DoD should seek to at least harmonize requirements between different IT security frameworks. Given the availability of FedRAMP advisory and assessment (3PAO) expertise in the marketplace, DoD should clarify the FedRAMP Equivalency memo to allow for a risk-based approach to managing POAMs.

3. Incident Reporting Requirements

In *Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements* (DFARS 252.204-7021), Section (b)(4) states that the Contractor shall "notify the Contracting Officer within 72 hours when there any lapses in information security or changes in the status of CMMC certificate or CMMC self-assessment levels during the performance of the contract." While DoD has stated that this clause is not intended to duplicate the incident reporting requirements in DFARS 252.204-7012, the phrase "lapses in information security" is vague and could become conflated with incident reporting. This could inadvertently create a new and redundant reporting for contractors. To avoid confusion and ensure that this remains a higher level directive related to the overall status of their CMMC level and certificate, ADI urges DoD to delete the words "lapses in information security" in Section (b)(4) so that it reads the Contractor shall "notify the Contracting Officer within 72 hours when there any changes in the status of CMMC certificate or CMMC self-assessment levels during the performance of the contract."

4. Waivers

[4] https://dodcio.defense.gov/Portals/0/Documents/Library/FEDRAMP-EquivalencyCloudServiceProviders.pdf
[5] https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

In the proposed rule, DoD does not state whether, or under which circumstances, waivers for CMMC 2.0 requirements would be available. During the three-year phase-in period, DFARS clauses may be included in some contracts but not others. If there is not a defined waiver process, agencies and contracting officers will default to inclusion of new DFARS clauses leading to much more condensed phase-in timeline. To address this issue, ADI urges DoD to create a formal waiver procedure that allows procurement officials to grant temporary exemptions if necessary.

5. Definition of "Senior Company Official"

In the proposed rule, DoD does not define the term "senior company official." Therefore, it is unclear who within a company is responsible for affirming in the Supplier Performance Risk System (SPRS) continuous compliance with the security requirements identified at 32 CFR part 170. While this term can be interpreted as the first level executive within the company, it is not clear. This could ultimately lead to inconsistencies in compliance and reporting across the CMMC 2.0 program. Therefore, ADI encourages the DoD to provide a clear definition of "senior company official" in the final rule.

6. Limited number of C3PAOs

To support the implementation of the CMMC 2.0 program, a sufficient number of Certified Third-Party Assessor Organizations (C3PAOs) will be required to conduct the necessary assessments. In the proposed rule, the DoD estimates that 10,340 entities will need a CMMC Level 2 (Advanced) Certificate by the end of the fourth year of CMMC 2.0 implementation. However, there are currently only 57 approved C3PAOs, which raises concerns about whether they are capable of meeting projected demand. Moreover, the proposed rule gives program offices the discretion to decide when exactly to implement CMMC 2.0 requirements during the program's phased rollout. Therefore, if many program offices decide to implement requirements at the same time, it could create a bottleneck of entities seeking certifications. To address this issue, the DoD should seek to increase the number of C3PAOs able to support CMMC 2.0 certification demand. Additionally, DoD should explore investing in new and innovative cybersecurity risk management techniques that include the use of NIST OSCAL and AI based models for assessing and streamlining assessments. In the meantime, DoD could give program offices more direction about how to not create such a bottleneck.

Thank you for allowing ADI to submit feedback. We look forward to continuing to partner with the Department of Defense to align contracting requirements to secure outcomes.

Sincerely,

The Alliance for Digital Innovation (ADI)