COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22203
codsia@codsia.org
www.codsia.org

CODSIA Case – 2020-007

November 30, 2020

Defense Acquisition Regulations System
Attn: Ms. Heather Kitchens
OUSD(A–S) DPC/DARS, Room 3B941
3060 Defense Pentagon
Washington, DC 20301–3060

Ref: Interim Rule for DFARS Case 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements

Dear Ms. Kitchens:

On behalf of the member associations of the Council of Defense and Space Industry Associations (CODSIA),[1] we are pleased to submit these comments on the interim rule amending the DFARS to implement new provisions and clauses titled, Assessing Contractor Implementation of Cybersecurity Requirements, published in the September 29, 2020, *Federal Register*.[2] The general methodology for DoD assessments in relationship to DoD CUI is a primary concern for CODSIA members. While we acknowledge that DoD should be able to access a contractor's facilities and systems, the Level 4 & 5 CMMC certifications should only be reserved for sensitive and mission critical areas (such as nuclear deterrence). Additionally, DoD should define new parameters warranting a high assessment requirement. While we generally support the interim rule, we also provide the following comments for your consideration.

DoD Assessment Processes and Procedures

Process improvements are needed as to how the results of self and DoD assessments will be operated, consumed, and protected. Prime contractors should be able to query a single source of records without undue risk or exposure to both government and industry stakeholders. The Supplier Performance Risk System (SPRS) capabilities are currently inadequate to meet the requirements of the rule. Additional considerations are

[1] CODSIA was formed in 1964 by industry associations with common interests in federal procurement policy issues at the suggestion of the Department of Defense. CODSIA consists of eight associations – Aerospace Industries Association (AIA), American Council of Engineering Companies (ACEC), Associated General Contractors (AGC), CompTIA, Information Technology Industry Council (ITI), National Defense Industrial Association (NDIA), Professional Services Council (PSC), and U.S. Chamber of Commerce. CODSIA's member associations represent thousands of government contractors nationwide. The Council acts as an institutional focal point for coordination of its members' positions regarding policies, regulations, directives, and procedures that affect them. A decision by any member association to abstain from participation in a particular case is not necessarily an indication of dissent.
[2] 85 Fed. Reg. 61505, September 29, 2020, available at https://www.govinfo.gov/content/pkg/FR-2020-09-29/pdf/2020-21123.pdf

required as Prime contractors should only be able to request potential and supporting subcontractors to present CMMC certificates of compliance.

Compliance & CMMC Certification at Time of Award
While requiring compliance and future certification at time of award is reasonable, flexibility should be provided for supply chain compliance and certification levels. In the majority of acquisitions, subcontracts in practice occur much later than the prime award. The award process, and the varied acquisition scenarios, should be reviewed to develop procedures and timeframes to allow for subcontractors to report/obtain a valid assessment and, upon CMMC finalization, the specified certification(s).

COTS Exception
While we encourage DoD to comply with 10 U.S.C. 2375 by exempting *all* commercial item procurements from Assessment and CMMC requirements, we strongly support the current exemption for COTS items. However, to reduce confusion and ensure consistency when implementing the CMMC COTS exemption, we urge DoD to issue department-wide guidance clarifying the definition of "COTS" for Assessment and CMMC purposes as FAR Part 2 Subpart 2.1 Section 2.101 Definitions specified as Commercially available off-the-shelf (COTS) item.

Cloud & International Reciprocity:
Many federal contractors have achieved compliance through equivalency in accordance with DFARS 252.204-7012 by implementing cybersecurity requirements under the Federal Risk and Authorization Management Program (FedRAMP). Other certifications may also be relevant to nonfederal systems and operational for governments, industries, applicable for global and in country operations based upon International Organization for Standardization (ISO), DoD's Cloud Computing Security Requirements Guide (CC SRG), the NIST Cyber Security Framework (CSF), and Risk Management Framework (RMF). To facilitate reciprocity, CMMC maturity levels must be clearly mapped to existing cybersecurity controls and frameworks. This mapping of equivalent certification levels to CMMC maturity levels should be stated in writing and through agreements used consistently throughout DoD and Government to demonstrate and indicate the use of the security controls satisfied through the security certification programs.

CMMC Recertification
With the phased, five-year implementation and ramp-up of the CMMC assessments and certification of contractor networks, there are significant scalability concerns, especially as they pertain to the possibility that C3PAO overextension will result in certification and recertification delays. Additionally, since Federal procurement cycles frequently cause RFP delays, which can further complicate the CMMC process, primes should be able to

apply for an extension if they can demonstrate that they requested an assessment, or reassessment, within a reasonable/specified amount of time. Since the threat is ever-changing, the DoD also needs to clarify the criteria, conditions, process, and timeline for CMMC recertification.

CMMC Level Requirements & Flexibility

The interim rule describes, in the Supplementary Information, alternatives and thresholds for Level 4 and Level 5. DoD should consider a "Flex" model for CMMC Level 4 & 5 practices that would augment a one-size-fits-all concept for a favorable risk-based management approach to cybersecurity. Contractors would be given the flexibility("Flex") to select the practices in order to employ tools, techniques, and processes to specifically detect and defend against Advanced Persistent Threats (APT) based upon architectural environments and dynamic threat models. The "Flex" model would also align with the tailoring statement documented in the Draft NIST Special Publication 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171 as "(t)here is no expectation that all of the enhanced security requirements will be selected by every agency."

Thank you for your attention to these comments. We welcome the opportunity to discuss them with you and the drafting team at your convenience. If you have any questions or need any additional information, please do not hesitate to contact CODSIA's lead on these comments, Jason Timm, Assistant Vice President, National Security Policy, Aerospace Industries Association. Jason may be reached at (571) 229-0661 or jason.timm@aia-aerospace.org.

Sincerely,

John Luddy
Vice President National Security
Aerospace Industries Association

Steve Hall
Vice President, Government Affairs
American Council of Engineering Companies

Jimmy Christianson
Regulatory Counsel

David Logsdon
Senior Director
CompTIA Federal Procurement Council

CODSIA Case – 2020-007

Associated General Contractors of America

Wesley P. Hallman
Senior Vice President for Policy
National Defense Industrial Association