ACEC
American Council of Engineering Companies

October 15, 2024

Ms. Heather Kitchens
OUSD(A&S) DPC/DARS
3060 Defense Pentagon
Washington, DC 20301-3060

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

Dear Ms. Kitchens:

The following comments are submitted on behalf of the American Council of Engineering Companies (ACEC) – the business voice of the U.S. engineering industry. Founded in 1906, ACEC is a national federation of 51 state and regional organizations representing nearly 5,500 engineering firms and nearly 600,000 engineers, surveyors, architects, and other specialists nationwide. 85% of our member companies have 100 employees or less and 74% of our member companies have 50 employees or less. ACEC member firms drive the design of America's infrastructure and built environment.

ACEC is pleased to provide input and seek clarifications on the proposed Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041) by the U.S. Department of Defense as published in the *Federal Register* on Thursday, August 15, 2024; Docket ID: DARS-2020-0034, RIN 0750-AK81.

Appropriately, these comments are due during National Cybersecurity Awareness Month. ACEC supports the goals of the Cybersecurity Maturity Model Certification (CMMC) Program. We support efforts to strengthen U.S. Department of Defense (DoD) cybersecurity practices and understand that companies who support DoD are critical partners in protecting information from malicious entities.

Program Methodology for CMMC Requirements

CMMC is proposing a phased approach to the implementation of CMMC requirements in contracts; however, the rule leaves those determinations up to the discretion of the program without transparent methodology on how the program should decide. By allowing discretion at the program level with no clear methodology or control method, it risks CMMC requirements rolling out sooner and in greater volumes than the Defense Industrial Base (DIB) and CMMC

Third-Party Assessor Organization (C3PAOs) may be able to support. Lack of a clear methodology could have the effect of cutting DIB companies out of competing for contracts and offering DoD best value. DoD estimates that 63% of DoD prime contracting entities would have to meet “Level 1” or at least 29,543 entities. These estimates do not include subcontractors.

This could also cause smaller businesses to exit the market because the contract requirements are increasing at an unsustainable rate surpassing their ability to invest in security practices to compete. Of the at least 29,543 entities estimated in the proposed rule, 69% of them are small businesses. Again, these estimates do not include subcontractors.

Specific consideration should be given to contracts for architect/engineering (A/E) services (40 U.S.C. 1101-1104 and P.L. 107-217). Problem solving is at the core of physical infrastructure design work. This requires innovative thinking and unique application of physical laws to specific challenges. Work is often done by teaming companies that bring specific expertise to be selected as the most qualified “offeror” for each individual project. The team works on portions of designs, sharing changes, approval processes, storing information, etc. using COTS information systems over the internet. With digital delivery becoming more commonplace and emerging technologies such as digital twins, some software can standardize engineering work in progress using scalable and customizable workflows without limiting the number of projects an organization can manage and without having to start over with new CAD applications. Since there are no established tools for sharing electronic information, verification falls on prime contractors. Conducting verifications adds considerable requirements on firms whose expertise is not information systems and rely on commercial software systems. This is compounded by the potential for CUI designated such after the fact. Further considerations include:

- The requirements under 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, are triggered when the contractor processes, stores, or transmits CUI on a covered contractor information system (the contractor's internal information system). This broad requirement has a significant impact on the ongoing operations of A/E firms that use unclassified information that DOD may require "control" of after work has been performed. The contract may include CMMC certification which the firms involved thought they were complying with, but unintentionally violated. Protections are needed. As described in this proposed rule, if there is a requirement for CMMC, then it applies to all information systems that process, store, or transmit FCI or CUI in performance of the contract.

ACEC recommends DoD publish the methodology by which programs determine the CMMC level and the timing of the certification requirement, this would ensure greater transparency and ability to negotiate with programs that might be overly aggressive in their desire to adopt CMMC and negatively impact DoD’s ability to extract a qualification-based selection. Special considerations for A/E services and fundamental research need to be considered and carefully implemented.

Contract Flowdown Requirements

Industry requests further clarification around the flowdown of CMMC requirements to subcontractors and the lack of a standardized mechanism for prime and subcontractors to verify the compliance of their subcontractors. In some cases, the prime and subcontractor could be subject to different CMMC Levels. In other cases, they could have multiple contracts requiring different levels. The prime and subcontractor also could be in a position where their roles are reversed—such that the subcontractor could be the prime and the prime could be a subcontractor in another contract—and the subcontractor could, and may, be forced to evaluate the other's compliance on other contracts. A prime and subcontractor could have multiple contracts where this occurs.

It is already difficult for some subcontractors and suppliers to comply with and implement NIST SP 800-171 controls. Making prime contractors responsible for oversight and verification of compliance of their entire defense supply chain will place substantial risk and liability on prime contractors that have neither the resources nor the ability or insight to adequately manage and effectively oversee subcontractor CMMC compliance on such a large scale and on a continual basis. We strongly encourage the DoD to explicitly clarify the relationship, roles, and responsibilities between the prime and subcontractor under the CMMC rule.

A lack of privity between prime contractors and lower-tier subcontractors and suppliers creates a barrier to collecting valuable information that will allow a prime to confirm that CUI is properly safeguarded. We note that a manual validation process will be cumbersome and may lead to oversights during the enforcement of 7021(b)(6). We see at least two possible solutions that could improve this process. The first is to create an automated tool that provides upper-tier suppliers with visibility into certification status without revealing supporting artifacts. This could entail allowing the prime to access assessments and attestations contained in the Supplier Performance Risk System (SPRS) concerning any subcontractor performing within the supply chain of the prime's government contract. The second option would be to limit the scope of 252.204-7021(b)(6) to direct suppliers without requiring enforcement throughout the entire supply chain. This is like the approach taken in 252.204-7021(d) and would flow down the enforcement responsibility to the most appropriate contracting tier.

Limited guidance leaves open many questions for both prime and subcontractors – with potential penalties of the False Claims Act as consequences. Companies cannot comply if they do not understand the rules and procedures. This ambiguity compromises the intent of the rule entirely.

Use Existing Processes

When DIB companies experience a security incident, they are already required to report it within 72 hours via the DIBNET portal, which then is supposed to notify all affected contracts. This process helps streamline and make more efficient the reporting process. By requiring the DIB company to individually notify each Contracting Officer, this new process risks slowing down the pace at which notifications can be made and consuming DIB company's time and resources that could be spent managing the lapse/incident. Similarly, a company's compliance with DFARS cybersecurity is managed via the SPRS website which government contracting officers

can check and monitor for supplier compliance in a one-stop-shop. The requirement to individually notify contracting officers about CMMC status will introduce extra work for little to no additional value, SPRS already solves this process.

Definition of Terms

ACEC respectfully asks for greater clarity on the following terms used in the rule and the activities required:

- The proposed rule introduces the term DoD unique Identifier, but it is unclear how these will be assigned, how they will be different from cage codes used today and how they will link back to company's cage codes. Risk introducing another layer of complexity and confusion, with unclear benefit / goal. ACEC recommends either sticking to the Cage Code linkages in SPRS used today for tracking compliance to DFARS 252.204-7020 or at least making it more clear how the DoD UI process will work and be used.

- The proposed rule uses the term "Contractor Information Systems" where previous guidance has used "Covered Contractor Information System," this again risk broadening the scope of applicability to system unrelated to CUI and FCI, such as COTS and SaaS. ACEC recommends the government narrowly define what the term "Contractor Information System" means or revert to the old term "Covered Contractor Information System."

- The use of the term "data" in the CFR does not clearly state how it defines and applies this term, which will cause confusion and potentially impact systems in scope, as that term could be interpreted broadly. ACEC recommends that the government narrowly define the categories of data to which the rule applies (e.g. CUI or FCI).

- Better clarify the intent of FCI and CUI. If the intent was to require all FCI handling to occur within the CUI-certified boundary, then this is largely inexecutable across the DIB and represents another significant expansion of requirements. ACEC recommends that the language be clarified to allow a contractor that only does some DoD work to continue to use their existing and compliant business systems for the processing of FCI and build an enclave at the higher security requirement level for CUI. This is both an important option to control costs and one that has been under construction broadly in the DIB based on existing guidance.

- The term "affirmation" has not been used in DoD contracts to date, but representations exist and are operational in federal contract administration and management by authoritative regulation. The rule introduces the requirement for an affirmation of continuous compliance with security requirements. However, it is unclear what is included in the affirmation and how it is to be measured. ACEC recommends eliminating the continuous affirmation aspect of this requirement and instead keep it as an affirmation at a single point in time such as an annual representation.

- The proposed rule introduces the term "lapse" in relation to cybersecurity and potential incidents, however the rule does not clearly define what constitutes a "lapse" which again

could lead to confusion and increase work activity from DIB companies. ACEC recommends harmonization with the existing DFARS 252.204-7021 clause.

Harmonization Across Government

DoD appears to have made no attempt to harmonize the proposed DFARS requirements with cybersecurity requirements proposed or required by other agencies, including the U.S. Department of Homeland Security's Critical Infrastructure Security Agency and the FAR Council – ignoring Congress' and the Administration's plans for cybersecurity regulatory harmonization and creating another area of frustration for contractors.

Because the U.S Government published the 146-page Cybersecurity Maturity Model Certification (CMMC) Program final rule today (October 15, 2024), which includes changes to part 32 CFR and which serves as a companion to this proposed rule, the comments hereunder do not reflect those part 32 CFR changes.

Invitation

ACEC would like to invite a suitable speaker from the U.S. Department of Defense to speak about the CMMC program with our member companies on a mutually agreed upon date via online seminar or in person. We frequently hold online seminars throughout the year and our Federal Agencies Winter Meeting is coming up in February 2025.

Thank you for your consideration of our industry's concerns and recommendations. We are committed to working with the U.S. Department of Defense to find cybersecurity solutions without significant business disruption and ensure a vibrant marketplace for all businesses.

Respectfully,

Bradley J. Saull
Vice President, Federal & International Programs
American Council of Engineering Companies (ACEC)