AMERICAN BAR ASSOCIATION
Public Contract Law Section

321 N. Clark Street
Chicago, IL 60654-7598
pubcontract@americanbar.org
ambar.org/pubcon



October 15, 2024

*Via Federal eRulemaking Portal*
*(https://www.regulations.gov)*

Defense Acquisition Regulations System
Office of the Undersecretary of Defense (A&S)
Defense Pricing and Contracting
3060 Defense Pentagon
Room 3B938
Washington, DC 20301-3060

**Re: Federal Acquisition Case 2019-D041 – Comments on Proposed Rule to Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements**

On behalf of the American Bar Association ("ABA") Public Contract Law Section, I am submitting comments in response to the Proposed Rule cited above. The Section consists of attorneys and associated professionals in private practice, industry, and government service. The Section's governing Council and substantive committees include members representing these three segments to ensure that all points of view are considered. By presenting their consensus view, the Section seeks to improve the process of public contracting for needed supplies, services, and public works.

The views expressed herein are presented on behalf of the Section. They have not been reviewed or approved by the House of Delegates or the Board of Governors of the ABA and, therefore, should not be construed as representing the position of the ABA.

## I. INTRODUCTION

The Section commends the Department of Defense (DoD) for the significant work completed to date to promote the need for better cybersecurity through assessments and the introduction of the Cybersecurity Maturity Model Certification (CMMC) program. 85 Fed. Reg. 61505 (Sept. 29, 2020). The Section appreciates the importance of adequately addressing cybersecurity to protect sensitive data in the information systems of defense contractors and their supply chains. Many members of the Section have worked hand-in-hand with

DoD to encourage a transparent and cooperative process to implement such effective cybersecurity. In this spirit, the Section has carefully reviewed the Proposed Rule and provides comments and proposed revisions for DoD's consideration before it issues a Final Rule.

The Section has a series of concerns and suggestions regarding the Proposed Rule, including the revisions to DFARS 252.204-7021, which provides for the acquisition requirements for assessing the implementation of the CMMC program for DoD's contractors and subcontractors. The concerns and suggestions are roughly organized across four topics: implementation, data and information systems, compliance and change management, and supply chain.

## II. COMMENTS ON IMPLEMENTATION

A. The proposed rule issued under Title 32 of the Code of Federal Regulations (CFR) contemplates that the CMMC program will be rolled out over a period of years. This gradual implementation will include the addition of this requirement during some option year contracts under Phases 2 or 3. *See* 32 CFR §170.3(e)(2)-(3). For option periods that are utilized after the implementation of the rule, the proposed regulations are not clear on how the contracting officer would determine which contractor information systems are applicable to the contract effort. *See, e.g.,* 48 CFR 204.7503(c)(1). The Section suggests that DoD adopt the language proposed in 48 CFR 204.7503(b)(2) that requires the contractor provide this information to DoD; specifically the DoD Unique Identifier (DoD UID) for each system the contractor is utilizing for contract performance that houses the relevant information.

B. In the proposed rule issued under Title 32 of the CFR, DoD provides a timeline for the implementation of the CMMC program and specifically states that third-party assessments (where applicable) will be required for all new contracts beginning six months after the implementation date of the rule. In the comments and responses to this proposed rule, DoD states that "[c]ontracting officers have the discretion to bilaterally incorporate the clause in contracts in effect prior to the effective date of the clause, with appropriate consideration." The Section is of the opinion that any such early implementation would make it difficult for prime contractors and their extensive supply chains to be compliant with the program without adequate warning. Despite the efforts of the Cyber Accreditation Body, there is approximately just one assessment team for every 700 contractors that will need an assessment. The creation of uncertainty in the marketplace could create a rush and an unnecessary bottleneck moving resources away from critical programs.

Because of this, the Section recommends identifying programs in advance that DoD would like to incorporate into the CMMC program to allow those contractors in that supply chain to engage with a third-party assessor and obtain a certification. To the extent that DoD does not intend to identify any particular programs prior to Stage 2, the Section suggests that DoD narrow the scope of programs in which it will require a certification to allow the supply chains for

each of the programs DoD identifies as critical to be able to access a third-party assessor.

## III. COMMENTS ON DATA AND INFORMATION SYSTEMS

A. The Section notes that the definition of Controlled Unclassified Information (CUI) in the Proposed Rule does not reflect how contractors receive CUI that requires safeguarding nor does the rule require the Government to mark or identify CUI when providing or instructing contractors to generate such information. These deficiencies are significant considering 32 CFR §§ 2002.4(c) and 2002.16(a), which set forth that non-executive branch entities receive CUI through a contractual arrangement. The guidance within DOD INSTRUCTION 5200.48 Section 5.3 also highlights the significance of the gaps in the CUI definition. Section 5.3 clarifies that contractors do not designate information as CUI based upon the general definition in 32 CFR §2002.4(h). Instead, the Government must mark information as CUI when provided and, for contractor-generated information, provide instructions on when such information is CUI and provide marking instructions for the same.

The Section further notes that the definition of Federal Contract Information (FCI) is only provided in FAR 4.1901 and is not included in the contract clause.

These definitional deficiencies create unnecessary ambiguity for contractors and subcontractors and potentially increase costs of compliance by encouraging contractors to adopt conservative interpretations as to which information systems to certify and to require subcontractors to exceed the minimum certification or assessment levels.

The Section suggests: (1) that the definition of CUI be revised to only include information that is marked; and (2) that a definition for FCI be added. The Section also suggests that there should be a mechanism for working with the contracting officer to establish whether information is properly categorized as FCI or CUI, especially for suppliers who may not receive FCI or CUI for a particular contract.

B. The Proposed Rule does not include a definition for, and does not use, the term covered defense information (CDI), which is defined in the existing clause DFARS 252.204-7012, and which is the basis for the safeguarding requirement in that existing clause and, in part, underpins the CMMC program. The Section is concerned that this lack of definitional alignment could create confusion and inconsistency, as it could imply that the scope of information on contractor information systems covered by the Proposed Rule is much larger than the scope of information on contractor information systems covered by the existing clause for CDI and FAR 52.204-21 for FCI. Such an interpretation would be contrary to the information provided during the rulemaking for 32 CFR Part 170 that indicates the scope of information covered by CMMC levels 1 and 2 are the same as the scope of information covered by FAR 52.204-21 and DFARS

252.204-7012 respectively. The Section suggests harmonizing the definitions, either by updating the definitions in the Proposed Rule or by updating the existing clause to eliminate the use of the term "covered defense information" and refer to all information needing safeguarding as DoD "Controlled Unclassified Information" using the same definition in the Proposed Rule. The Section emphasizes the above recommendation to limit CUI to marked information and the importance of the language in the proposed clause in 252.204-7021(b)(2) that scopes the requirement to "information systems, used in performance of the contract, that process, store, or transmit Federal contract information (FCI) or controlled unclassified information (CUI)".

C. In 252.204-7021(b)(2), the Proposed Rule requires contractors to maintain the CMMC level required by the contract for the duration of the contract for all information systems that process, store, or transmit FCI or CUI. The Section is concerned that this language is confusing and could be interpreted to mean that if the solicitation requires a CMMC level 2 or higher, then even the contractor's systems that process, store, or transmit only FCI would also require CMMC level 2. This interpretation would be at odds with the CMMC program rule at 32 CFR Part 170, which indicates that an information system that processes only FCI would require CMMC level 1 and allows contractors to use isolated "enclaves" within their environments to store FCI or CUI. The Section recommends bringing the Proposed Rule language in line with the CMMC program rule and making clear that information systems processing FCI but not CUI only need CMMC level 1.

D. In 252.204-7021(b)(3), the Proposed Rule appears to require the safeguarding of contractor information systems that are not used in performance under a contract but nonetheless might process or transmit FCI or CUI. The Section is concerned that this requirement is not addressing a procedure to implement CMMC but is instead requiring limits on the use of contractor information systems that may not be subject to CMMC. The Section suggests deleting this requirement from the Proposed Rule and considering adding an appropriate variation to the existing clause DFARS 252.204-7012, which addresses safeguarding and cyber incident reporting for CDI. Alternatively, the Section suggests aligning the scoping of this requirement to the CMMC program rule at 32 CFR Sec.170.19.

E. In 252.204-7021(b)(3), the Section is concerned with the lack of a specific definition of the word "data" in the requirement to only process, store, or transmit data on information systems that have a CMMC certificate or CMMC self-assessment. This lack of specificity creates ambiguity and overly broadens the requirement, as it could imply that contractors would be required to use CMMC-certified systems for all information and data stored within their systems, even those that may not actually be subject to CMMC. If this requirement is not deleted as recommended above, alternatively the Section suggests replacing "data" with a defined term, such as "FCI or CUI", to limit the scope of the requirement.

F. The Proposed Rule requires the contractor to submit to the contracting officer the DoD unique identifier(s) (UID(s)) issued by the Supplier Performance Risk System (SPRS) for contractor information systems that will process, store, or transmit FCI or CUI during performance of the contract. This requirement is unclear about whether a prime contractor must provide UIDs only for the prime contractor's own information systems that meet this definition, or also for the information systems of prime contractor subcontractors/suppliers that meet this definition. Because the Proposed Rule instructs prime contractors to exclude certain paragraphs regarding DoD UID requirements when flowing the substance of the clause to subcontractors, the Section presumes the former interpretation is the correct one but nonetheless recommends that the Proposed Rule language be revised to make that clearer. The Section also recommends clarifying the scope of what constitutes an "information system" regarding the DoD UID requirements, as it could refer to individual information systems or an amalgamation of information systems that are used to process FCI and/or CUI. The Section recommends expressly permitting contractors to define the scope of the "information system" that applies to a given DoD UID requirement, similar to the approach used by the Cybersecurity & Infrastructure Security Agency in the Common Form for Secure Software Development Framework-related attestations.

## IV. COMPLIANCE AND CHANGE MANAGEMENT

A. Use of Plans of Actions and Milestones (POA&Ms) for Maintaining Ongoing Compliance

The Proposed Rule requires contractors to achieve, at time of award, a CMMC certificate or CMMC self-assessment at the level specified in the solicitation, or higher. This is understandable as part of the rule.

However, there also is language in the Proposed Rule suggesting that contractors can never have temporary deficiencies in compliance thereafter. Specifically, "[c]ontractors are required to maintain a current CMMC certificate or CMMC self-assessment at the specified level, if required by the contract, task order, or delivery order, throughout the life of the contract, task order, or delivery order." Perfect compliance is not a standard that any organization (including DoD) can meet on its information systems.

The Final Rule should clarify that contractors may continue to rely on POA&Ms to address newly discovered risks or system flaws or when there are changes to the information systems that lead to temporary deficiencies. *See* NIST SP 800-171r2 (3.12.2). Because POA&Ms are part of the NIST SP 800-171 framework, contractors should have the latitude to continue to adopt POA&Ms without being considered by DoD to have fallen out of "continuous compliance." Indeed, POA&Ms may be needed to address deficiencies or changes that in some cases arise outside the contractor's control. Without permitting contractors to use POA&Ms in this manner, the alternative may be for contractors to ignore new risks or system vulnerabilities to remain eligible for defense contracts. Such an

approach would not adequately protect information systems with CDI and thus would defeat the whole purpose of DoD's cybersecurity compliance regime.

Without the mechanism afforded by POA&Ms, as noted, contractors that have temporarily fallen out of compliance, which can often result from circumstances outside the contractor's control, may be precluded from winning new business. This also could mean reduced competition and higher prices for DoD. In addition, DoD risks losing critical and innovative suppliers in the defense supply chain needed to help deliver products and services to DoD components. See also Section V of this letter regarding POA&Ms and commercial subcontractors.

The Section recommends a Final Rule that allows limited use of POA&Ms (beyond the Conditional Certification process contemplated in 32 CFR Part 170) for managing changes to contractor information systems while maintaining compliance.

B. Meaning of Changes

The Proposed Rule requires contractors to affirm their continuous compliance with CMMC requirements "when changes occur" that could affect their compliance status. However, the rule does not define what constitutes a change, or provide any procedures or criteria for determining when a change is significant enough to warrant an affirmation. This could create uncertainty and inconsistency among contractors and contracting officers and impose unnecessary administrative burdens on both parties. For example, if a contractor makes a minor or routine modification to its information system to address a security vulnerability or to improve its performance, would that trigger an affirmation requirement? What if a contractor merges with or acquires another entity that has a different or lower CMMC level? How would a contractor document and communicate its affirmation to the contracting officer? The Section suggests adding definitions and procedures to provide clarity and guidance around change management, and to align them with existing best practices, such as the Federal Risk and Authorization Management Program (FedRAMP) Continuous Monitoring framework.

C. Change Notification

The Proposed Rule requires contractors to notify the contracting officer if there is a change in the status of their CMMC certificate or CMMC self-assessment level during performance of the contract. *See* 252.204-7021(b)(4). However, there is also a requirement in 252.204-7021(b)(5) to affirm continuous compliance in the event of a change in compliance status. The Section is concerned about this apparent duplicative reporting requirement. It is also unclear how the contracting officer would use or verify the information, which suggests that the information collected might have limited utility to the Government. Given the numerous security-related reporting requirements that contractors are increasingly subject to under state, federal, or foreign privacy and information

security laws and regulations, the Section emphasizes the importance of streamlining and simplifying these requirements wherever possible. The Section recommends consolidating these two requirements into a single reporting requirement, and providing more guidance on what constitutes a change in status for purposes of notifying the contracting officer.

D. Meaning of Lapses

The Proposed Rule requires contractors to report "any lapses in information security" within 72 hours to the contracting officer. However, the term "lapses" is undefined and ambiguous, and could encompass a wide range of incidents or events that may not be relevant or material to the Proposed Rule's objectives. The requirement also fails to specify what kind of information (FCI, CUI, or other) is subject to reporting, and lacks a definition of information security. As drafted, the requirement is not necessarily limited to information covered by the Proposed Rule and could create confusion and inconsistency among contractors and contracting officers. Moreover, it is unclear when the 72-hour period for the notification begins, and whether it is triggered by the discovery or the occurrence of the lapse. In addition, this requirement seems to overlap with existing reporting obligations under DFARS 252.204-7012 and the Cyber Incident Reporting for Critical Infrastructure Act of 2022, as amended, which already address incident response and information sharing for cyber incidents affecting DoD information systems or networks. The Section recommends deleting this provision, or at least clarifying the scope, definition, and timing of the reporting obligation, and harmonizing it with existing requirements.

E. Reporting Lapses by Subcontractors

The requirement in the Proposed Rule to report any lapses in information security or changes in CMMC status to the contracting officer could pose significant challenges for prime contractors who may not have direct visibility or control over their subcontractors' information security practices or CMMC compliance. It is unclear if the prime contractors must report to the contracting officer within the same 72-hour period as the subcontractors, or if they have additional time to do so. The Section recommends the Final Rule clarify whether subcontractors must report directly to the contracting officer or through their prime contractors, and whether prime contractors have any additional time or flexibility to report on behalf of their subcontractors. If subcontractors must report directly to the contracting officer, then the Section suggests adding guidance for how the subcontractor would obtain the contracting officer's contact information from the prime contractor.

F. Senior Company Official

The Proposed Rule states in the preamble that the affirmation of continuous compliance must be made by a senior company official and refers to a definition of "senior company official" at 32 CFR 170.4. However, there is no

definition of "senior company official" at 32 CFR 170.4, and the term does not appear in the proposed DFARS 252.204-7021 clause itself. This creates confusion and uncertainty about who is authorized and responsible for making the affirmation and what qualifications or credentials they must have. Moreover, the term "senior company official" is vague and arbitrary and does not reflect the diversity and complexity of organizational structures and roles among contractors. There are numerous examples of FAR and DFARS clauses that require contractors to make various representations or certifications as to their compliance without specifying that such certification be made by a "senior company official." For example, FAR 52.204-24 requires contractors to make certain representations regarding certain telecommunications and video surveillance services when making an offer. Similarly, DFARS 252.204-7019 requires contractors to have a current NIST SP 800-171 derived assessment for covered contractor information systems when submitting offers and includes a mechanism to allow contractors to submit self-representations of such assessments to the Government, without requiring a "senior company official" affirmation for each assessment. The Section recommends removing the reference to "senior company official" from the preamble and allowing contractors to designate an appropriate and qualified individual within their organization to make the affirmation of continuous compliance.

## V. SUPPLY CHAIN

### A. Cost and Resource Burden on Small Businesses

The Proposed Rule imposes significant financial and resource burdens on small businesses within the defense industrial base (DIB). Many small businesses lack the necessary infrastructure or capital to implement the required cybersecurity measures. While the Section recognizes the importance of protecting CUI throughout the DoD supply chain, inattention to this issue could cause small business suppliers to opt out of performing DoD contracts either directly with DoD or through supply chains. This could, in turn, shrink DoD's supply base and increase costs to the Government. Moreover, large business prime contractors will have difficulty fulfilling contract requirements.

To address this concern, the Government should consider providing financial and technical support to small businesses that have difficulty meeting CMMC standards including, for example, an assistance program connecting small businesses with C3PAO's at reduced rates. One model for providing financial assistance could be the technical and business assistance (TABA) funding available under the Small Business Innovation Program.

The Government may also consider allowing subcontractors providing commercial products or commercial services to use POA&Ms to achieve a CMMC Level 2 self-certification because this would provide a stepping stone for commercial companies that are likely to handle CUI in the future.

### B. Impact of Flowdown Requirements

The Proposed Rule requires prime contractors to flow down CMMC requirements to all subcontractors, regardless of their size or the nature of their contract work. It also requires prime contractors to flow it to any suppliers that will be handling CUI.

This flow down requirement assumes a level of certainty about the information being flowed down to the subcontractor. In reality, particularly at the beginning of contract performance, when subcontracts are negotiated, prime contractors do not know whether, and to what extent, a particular subcontractor will need to store, process, or maintain CUI during contract performance. This issue is compounded by the Government's inconsistent marking of CUI. In order to address this uncertainty, prime contractors often have no choice but to flow down requirements based on what could occur at the subcontractor level – resulting in an unnecessarily broad scope of requirements and an undue burden on subcontractors. For instance, if a subcontractor's scope of work does not contemplate needing CUI, the prime contractor may still require a CMMC Level 2 certification based on the possibility of CUI being shared during contract performance.

There are several ways that the Government could help contractors deal with this otherwise inevitable problem:

- Include a statement in DFARS 252.204-7012(m) (or elsewhere, as appropriate), explaining that flow down of a CMMC Level 2 is not required when there is not a present need or realistic expectation that the subcontractor will handle CUI and, thus, prime contractors should default to requiring a Level 1 self-assessment unless, and until, there is a need for a subcontractor to access CUI.

- Allow and encourage the use of information sharing agreements between prime and subcontractors that limit the sharing of CUI or explain how CUI will be handled during contract performance.

- Provide a mechanism for subcontractors to seek review of unnecessarily high CMMC certification level requirements imposed by prime contractors including, for example, a mechanism to request a variance that parallels DFARS 252.204-7012(m)(2)(i).

- Require contracting officers to coordinate closely with prime contractors at various phases of contract performance for the purpose of aligning on the sharing of CUI. This would further collaboration between the Government and its contractors to address compliance with this important requirement, and support contractors that are doing their best to encourage compliance throughout their supply chain. It will also help address the inconsistent marking of CUI by Government officials and the anticipated default to requiring CMMC Level 2.

C. <u>Requirements of Suppliers</u>

The Proposed Rule contemplates the flow down of CMMC requirements to suppliers, not just subcontractors. While understandably the Government wants suppliers to protect CUI with the same level of security as companies directly within its supply chain, this places an undue burden on industry and could result in companies that do business with DoD having less options in their supply chain. This would particularly strain small businesses. For example, companies that need to share CUI with suppliers such as accounting and law firms, could only do so if those firms accept a flow down even if those firms are not directly in the DoD supply chain.

To address this issue, the Section suggests clarifying that while suppliers need to store, process, or transmit CUI on IT systems compliant with NIST SP 800-171, they are not otherwise subject to the many requirements placed on contractors. This would allow such firms to create enclaves for storing this information, which would be less burdensome and less impactful on the supply chain than requiring full compliance with the DFARS rule.

D. Level Required Of Subcontractors

As drafted, the Proposed Rule is ambiguous with respect to whether the CMMC level is determined based upon the program/contract at issue, or the data that will be shared with companies throughout the supply chain. For example, if a contract contains a CMMC Level 3 requirement, must a company supplying relatively insignificant widgets still be under subcontract with a CMMC Level 2 requirement? To assist with this issue, the Government should consider providing additional guidance in the rule (i.e., in DFARS 252.204-7012(d)(2)) as to how a contractor should identify and mark data that will be shared with subcontractors and suppliers. Moreover, as noted above, the Government should also require routine coordination between the Contracting Officer and contractor on this important issue.

## VI. CONCLUSION

The Section appreciates the opportunity to provide these comments and is available to provide additional information or assistance as you may require.

Sincerely,
/s Jason N. Workmaster
Chair, Section of Public Contract Law

cc:
Daniel Chudd
Sheila A. Armstrong
Amy Conant Hoang
Brad Jorgensen
Patricia Hale Becker

Council Members, Section of Public Contract Law
Co-Chairs, Cybersecurity, Privacy, and Emerging Technology Committees
Eric S. Crusius
George E. Petel