6001-FR

DEPARTMENT OF DEFENSE

Defense Acquisition Regulations System

48 CFR Parts 204, 212, 217, and 252

[Docket DARS-2020-0034]

RIN 0750-AK81

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

AGENCY: Defense Acquisition Regulations System, Department of Defense (DoD).

ACTION: Proposed rule.

SUMMARY: DoD is proposing to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to incorporate contractual requirements related to the proposed Cybersecurity Maturity Model Certification 2.0 program rule, Cybersecurity Maturity Model Certification Program. This proposed DFARS rule also partially implements a section of the National Defense Authorization Act for Fiscal Year 2020 that directed the Secretary of Defense to develop a consistent, comprehensive framework to enhance cybersecurity for the U.S. defense industrial base.

DATES: Comments on the proposed rule should be submitted in writing to the address shown below on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**, to be considered in the formation of a final rule.

ADDRESSES: Submit comments identified by DFARS Case 2019-D041, using either of the following methods:

o *Federal eRulemaking Portal*: *https://www.regulations.gov*. Search for DFARS Case 2019-D041. Select "Comment" and follow the instructions to submit a comment. Please include "DFARS Case 2019-D041" on any attached documents.

o *Email*: *osd.dfars@mail.mil*. Include DFARS Case 2019-D041 in the subject line of the message.

Comments received generally will be posted without change to *https://www.regulations.gov*, including any personal information provided. To confirm receipt of your comment(s), please check *https://www.regulations.gov*, approximately two to three days after submission to verify posting.

FOR FURTHER INFORMATION CONTACT: Ms. Heather Kitchens, telephone 571-296-7152.

SUPPLEMENTARY INFORMATION:

I. Background

DoD is proposing to revise the DFARS to implement the contractual requirements related to the Cybersecurity Maturity Model Certification (CMMC) 2.0 program, published in the **Federal Register** as a proposed rule affecting 32 CFR part 170 on December 26, 2023, at 88 FR 89058. CMMC 2.0 provides a framework for assessing contractor implementation of cybersecurity requirements and enhancing the protection of unclassified information within the DoD supply chain. This proposed DFARS rule also partially implements section 1648 of

the National Defense Authorization Act for Fiscal Year 2020 (Pub. L. 116-92), which directed the Secretary of Defense to develop a consistent, comprehensive framework to enhance cybersecurity for the U.S. defense industrial base no later than February 1, 2020.

On September 29, 2020, an interim rule under DFARS Case 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements, was published in the **Federal Register** at 85 FR 61505, effective November 30, 2020. On November 17, 2021, the notice, "Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward" was published in the **Federal Register** at 86 FR 64100 to suspend the CMMC 1.0 pilot efforts. The purpose of suspending the CMMC 1.0 pilot efforts was to allow for development of CMMC 2.0. On December 26, 2023, DoD published in the **Federal Register** at 88 FR 89058 a proposed CMMC 2.0 program rule, Cybersecurity Maturity Model Certification Program, to propose the establishment of the CMMC 2.0 program requirements at 32 CFR part 170.

II. Discussion and Analysis

The proposed changes to the existing DFARS language are primarily to: (1) add references to the CMMC 2.0 program requirements proposed at 32 CFR part 170; (2) add definitions for controlled unclassified information (CUI) and DoD unique identifier (DoD UID) to the subpart; (3) establish a solicitation provision and prescription; and (4) revise the existing clause language and prescription.

DoD is implementing a phased rollout of CMMC. Over a three-year period CMMC will be phased in based on the CMMC 2.0 program requirements identified at 32 CFR part 170. The clause at DFARS 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements, is prescribed for use in solicitations and contracts that require the contractor to have a specific CMMC level, including solicitations and contracts using Federal Acquisition Regulation (FAR) part 12 procedures for the acquisition of commercial products and commercial services, excluding acquisitions exclusively for commercially available off-the-shelf (COTS) items. In order to implement the phased rollout of CMMC, inclusion of a CMMC requirement in a solicitation during this time period will be determined by the program office or requiring activity after consulting the CMMC 2.0 requirements at 32 CFR part 170. During the phase-in period, when there is a requirement in the contract for CMMC, CMMC certification requirements must be flowed down to subcontractors at all tiers, when the subcontractor will process, store, or transmit Federal contract information (FCI) or CUI, based on the sensitivity of the unclassified information flowed down to each of the subcontractors in accordance with the proposed CMMC 2.0 requirements to be established at 32 CFR part 170 (see the proposed rule published December 26, 2023, at 88 FR 89058).

After the phase-in period, CMMC will apply to all DoD solicitations and contracts, including those for the acquisition

of commercial products or commercial services (except those exclusively for COTS items), valued at greater than the micro-purchase threshold that involve processing, storing, or transmitting FCI or CUI. When a CMMC level is included in the solicitation or contract, contracting officers will not make award, exercise an option, or extend the period of performance on a contract, if the offeror or contractor does not have the results of a current certification or self-assessment for the required CMMC level, and an affirmation of continuous compliance with the security requirements to be identified at 32 CFR part 170, in the Supplier Performance Risk System (SPRS) for all information systems that process, store, or transmit FCI or CUI during contract performance. Furthermore, CMMC certification requirements must be flowed down to subcontractors at all tiers when the subcontractor will process, store, or transmit FCI or CUI, based on the sensitivity of the unclassified information flowed down to each of the subcontractors in accordance with the proposed CMMC 2.0 requirements to be established at 32 CFR part 170 (see 88 FR 89058).

A. Proposed Rule Changes

This proposed rule includes amendments to DFARS 204.7502, Policy. These amendments require at the time of award the results of a current CMMC certificate or CMMC self-assessment, at the level required, for all information systems that process, store, or transmit FCI or CUI during contract performance, when a CMMC level is included in the solicitation.

The proposed rule also adds a requirement at DFARS 204.7503, Procedures, for contracting officers to work with the program office or requiring activity to verify in SPRS, prior to awarding a contract, exercising an option, or when new DoD UIDs are provided, that: (1) the results of a current CMMC certificate or current CMMC self-assessment at the level required by the solicitation, or higher, are posted in SPRS for each DoD UID applicable to each of the contractor information systems that will process, store, or transmit FCI or CUI and that will be used in performance of the contract; and (2) the apparently successful offeror has a current affirmation of continuous compliance with the security requirements identified at 32 CFR part 170 in SPRS for each DoD UID applicable to each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract.

The proposed rule also adds a definition at DFARS 204.7501 for use only in the subpart for the term CUI based on the 32 CFR 2002 definition of CUI. Definitions for current (as it relates to CMMC) and DoD UID are also added.

This proposed rule includes a new DFARS provision, 252.204-7YYY, Notice of Cybersecurity Maturity Model Certification Level Requirements, to provide notice to offerors of the CMMC level required by the solicitation and of the CMMC certificate or self-assessment results that are required to have been posted in SPRS by the apparently successful offeror prior to award, unless

electronically posted. Offerors post CMMC Level 1 and Level 2 self-assessments into SPRS. Level 2 certificate assessment results will be electronically transmitted to SPRS by the third-party assessment organization (see the proposed rule published at 88 FR 89058, in the proposed text at 32 CFR 170.17 for details on CMMC Level 2 certification assessment requirements). Level 3 certificate assessment results will be electronically transmitted to SPRS by the DoD assessor (see the proposed rule published at 88 FR 89058, in the proposed text at 32 CFR 170.18 for details on CMMC Level 3 certification requirements).

Apparently successful offerors are also required to provide, at the contracting officer's request, the DoD UIDs issued by SPRS for the contractor information systems that will process, store, or transmit FCI or CUI during contract performance. SPRS will issue DoD UIDs to offerors in connection with their CMMC self-assessments and CMMC certificates. Apparently successful offerors will need to specify which DoD UIDs are applicable to the contractor information systems that will process, store, or transmit FCI or CUI during contract performance.

This proposed rule at DFARS 204.7504 adds the prescription for the new DFARS solicitation provision, 252.204-7YYY, Notice of Cybersecurity Maturity Model Certification Level Requirements. DFARS 252.204-7YYY is prescribed for use in solicitations that include the clause at 252.204-7021. The provision includes language identifying the CMMC level required for the contract and notifies offerors that the apparently successful offeror

will not be eligible for award of a contract, task order, or delivery order resulting from the solicitation in which the provision appears, if the apparently successful offeror does not have the results of a current CMMC certificate or self-assessment entered in SPRS (*https://piee.eb.mil*) at the CMMC level required by the provision and an affirmation of continuous compliance with the security requirements identified at 32 CFR part 170 in SPRS for each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract.

This proposed rule includes changes to the clause at DFARS 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement, to:

- Add definitions at paragraph (a) for Cybersecurity Maturity Model Certification, current (as it relates to CMMC), and DoD UID, and remove the scope statement.
- Require the contractor to have and maintain the requisite CMMC level for the life of the contract.
- Require the contractor to submit to the contracting officer the DoD UID(s) issued by SPRS for contractor information systems that will process, store, or transmit FCI or CUI during performance of the contract.
- Require the contractor to complete and maintain on an annual basis, or when security changes occur, the affirmation of continuous compliance with the security requirements identified at 32 CFR part 170. The affirmation of continuous compliance is

made by a senior company official (see definition of "senior company official" at 32 CFR 170.4 in the proposed rule published at 88 FR 89058) to affirm that its CMMC self-assessment of CMMC certification for each DoD UID applicable to the contractor information systems that process, store, or transmit FCI or CUI during contract performance remains current and the information system(s) covered by the CMMC self-assessment or CMMC certificate continue to be in compliance with the security requirements identified at 32 CFR 170.

- Require the contractor to notify the contracting officer of any changes in the contractor information systems that process, store, or transmit FCI or CUI during contract performance and to provide the corresponding DoD UIDs for those contractor information systems to the contracting officer. The contractor is required to provide the DoD UIDS to the contracting officer so the Government can review associated CMMC certificate or CMMC self-assessment results and contractor affirmations of continued compliance in SPRS for those additional contractor information systems.

- Require the contractor to ensure that its subcontractors also have the appropriate CMMC level prior to awarding a subcontract or other contractual instruments. This requirement is included in the clause at DFARS 252.204-7021, paragraph (d), which tells contractors when to flow the clause down to subcontractors.

- Require the contractor to include the requirements of the clause in subcontracts or other contractual instruments. The purpose of the clause is to ensure suppliers at all tiers are in compliance with the security requirements identified at 32 CFR part 170 when there is a requirement for CMMC in the contract, if applicable based on the information that is being flowed down. The CMMC program requirements related to the CMMC level required for suppliers is based on the information that is being flowed down, and those requirements are defined in the Title 32 CFR CMMC Program proposed rule.

The proposed rule also adds language to the clause at DFARS 252.204-7021 to incorporate a requirement for contractors to only transmit data on information systems that process, store, or transmit FCI or CUI during contract performance that have a certification at the CMMC level required by the contract. In addition, the contractor will be required to notify the contracting officer if there are any lapses or changes in CMMC certification levels that affect the requirements for information security during contract performance. The clause will also include language identifying the CMMC level required by the contract.

This proposed rule also includes revisions to the clause prescription at DFARS 204.7504 to apply the clause at DFARS 252.204-7021 to solicitations and contracts, task orders, or delivery orders that require the contractor to have a specific CMMC level, including solicitations and contracts using FAR part

12 procedures for the acquisition of commercial products and commercial services, except for solicitations and contracts solely for the acquisition of COTS items.

DoD considered three alternatives for the timing of the requirement to achieve a CMMC 2.0 level certification in the development of this proposed rule, weighing the benefits and risks associated with requiring CMMC 2.0 level certification: (1) at time of proposal submission; (2) at time of award; or (3) after contract award. DoD ultimately adopted the second alternative to require certification at the time of award. The drawback of the first alternative (i.e., at time of proposal submission) is the increased risk for offerors since they may not have sufficient time to achieve the required CMMC certification. The drawback of the third alternative (i.e., after contract award) is the increased risk to DoD with respect to the schedule and uncertainty due to the possibility that the contractor may be unable to achieve the required CMMC level in a reasonable amount of time given their current cybersecurity posture. This potential delay would apply to the entire supply chain and prevent the appropriate flow of FCI and CUI to the contractor and subcontractors.

This proposed rule also includes the following conforming changes:

- Makes references to the CMMC 2.0 program requirements by incorporating the citation for 32 CFR part 170 throughout the text of the proposed rule.

- Amends the list in DFARS 212.301 of solicitation provisions and contract clauses that are applicable for the acquisition of commercial products and commercial services to include the new provision at DFARS 252.204-7YYY, Notice of Cybersecurity Maturity Model Certification Level Requirements. The clause at DFARS 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements, is already included in this list from the prior interim rule under this DFARS Case 2019-D041.

- Amends DFARS 217.207, Exercise of Options, to advise contracting officers that when CMMC is required in the contract, an option may only be exercised after verifying in SPRS that the contractor has the required affirmation(s) of continuous compliance with the security requirements identified at 32 CFR part 170 and has posted the results of a current CMMC certificate or CMMC self-assessment at the level required by the contract, or higher. The text refers contracting officers to DFARS 204.7503(c) for complete details regarding these requirements.

B. Analysis of Public Comments in Response to the Interim Rule

This proposed rule follows the publication of an interim rule under this DFARS Case 2019-D041, which received over 750 public comments. Although this proposed rule does not finalize the interim rule, it responds to the public comments received and anticipates that these responses will facilitate the public's understanding of this proposed rule. Only comments submitted in

response to the interim rule as it relates to the contractual requirements are discussed below. The technical and programmatic comments on CMMC 1.0 are being handled in the CMMC program rule affecting 32 CFR part 170. In addition to technical and programmatic comments, the comments related to the CMMC cost analysis are also being addressed under the CMMC program rule affecting 32 CFR part 170. It should also be noted that any comments related to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 DoD Assessment methodology will be addressed under a separate DFARS Case 2022-D017, NIST SP 800-171 DoD Assessment Requirements. A discussion of the comments is provided as follows:

1. Small Business Impact

Comment: Several respondents requested more information on the impact to small entities from CMMC.

Response: As described in the regulatory flexibility analysis in section VI of this preamble, the phased roll-out of CMMC over three years is intended to mitigate the impact of CMMC on contractors including small entities and is only expected to apply to 1,104 small entities in year one. In addition, the provision and clause in this proposed rule exempt contracts that are exclusively for COTS items.

2. Requirement for CMMC

Comment: Several respondents inquired about how contractors will know there is a requirement to have CMMC certification.

Response: As stated in this proposed rule, if there is a requirement for a specific CMMC level, the CMMC requirement will be identified in the DFARS solicitation provision 252.204-7YYY, Notice of Cybersecurity Maturity Model Certification Level Requirements. In addition, the DFARS contract clause 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements, will be included in the contract.

3. CMMC Application to Other Transaction Agreements (OTAs)

Comment: Many respondents asked whether CMMC will apply to OTAs.

Response: Applicability to OTAs is outside the scope of this DFARS rule, as the DFARS does not provide coverage of OTA requirements. If the program office or requiring activity identifies a need to include a CMMC requirement in an OTA, it will be included in the solicitation and resulting agreement.

4. Application to Foreign Suppliers for CMMC

Comment: Many respondents commented on whether CMMC will apply to foreign suppliers.

Response: If the program office or requiring activity identifies a need to include a CMMC requirement in a contract, it will be included in the solicitation and resulting contract unless the contract is exclusively for COTS items. The proposed rule does not exempt foreign suppliers from CMMC requirements.

5. CMMC and NIST SP 800-171 DoD Assessment Requirements

Comment: Many respondents questioned how CMMC and the NIST SP 800-171 requirements will interact and if one requirement will be used for the other.

Response: As described in the interim rule at DFARS 204.7501(c), the CMMC assessments will not duplicate efforts from any other comparable DoD assessment, except for rare circumstances when a reassessment may be necessary, for example, when there are indications of issues with cybersecurity and/or compliance with CMMC requirements.

6. CMMC Application to Broad Agency Announcements (BAAs)

Comment: Many respondents inquired whether CMMC will apply to BAAs.

Response: If the program office or requiring activity identifies a need to include a CMMC requirement in a contract, it will be included in the solicitation and resulting contact. The proposed rule prescribes the CMMC clause at 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements, for use in solicitations and contracts, task orders, and delivery orders that require the contractor to have a specific CMMC level, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, except those solely for the acquisition of COTS items.

7. Duplication of DFARS Clause 252.204-7012 and DFARS Clause 252.204-7021

Comment: A respondent commented on whether DFARS clause 252.204-7012 and DFARS clause 252.204-7021 duplicate one another.

Response: These clauses are not duplicative as they have distinct purposes. DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, levies cybersecurity requirements on contractors, and DFARS clause 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements, levies a requirement for an assessment of how well a contractor is meeting those cybersecurity requirements specified in 252.204-7012.

8. Uniform Definition of CUI

Comment: A respondent commented that there should be a uniform definition of CUI.

Response: This proposed rule adds a definition for use in subpart 204.75 for the term "controlled unclassified information." The definition is based on the definition of CUI at 32 CFR 2002.

9. Uniformity and Consistency

Comment: Many respondents commented that the final rule should provide uniformity and consistency.

Response: This proposed rule does not conflict with other regulations.

10. Applicability to Contracts at or Below the Simplified Acquisition Threshold

Comment: Many respondents commented that there should be clarification as to whether this rule applies to contracts at or below the simplified acquisition threshold.

Response: As described in section III of this preamble, this proposed rule applies to contracts at or below the simplified acquisition threshold, but not to purchases at or below the micro-purchase threshold.

11. Expected Cost Impact and Benefits

Comment: Several respondents commented that the interim rule for 2019-D041 had a cost analysis that lacked a basis for the analysis.

Response: The Regulatory Impact Analysis associated with this proposed rule only includes a cost analysis of the contractual requirements associated with this proposed rule. The rule for the CMMC Program affecting 32 CFR part 170 contains the expected cost impact and benefits of technical requirements associated with CMMC. Any comments on the cost estimates of technical or programmatic requirements related to the CMMC Program should be directed to the proposed rule affecting 32 CFR part 170.

12. Applicability to COTS - Define Exclusively COTS

Comment: Many respondents commented that there needs to be a definition for "exclusively COTS".

Response: As described in this preamble, this proposed rule does not apply to awards that are exclusively for COTS items. The term "commercially available off-the-shelf (COTS) item" is defined at FAR 2.101, so any awards that are exclusively for

items falling within that FAR definition would be considered "exclusively COTS" awards.

13. Timing of CMMC Certification

Comment: Many respondents recommended that the CMMC certification timing be delayed until after award, or that it should be made more flexible.

Response: The CMMC policy identified in the CMMC 2.0 proposed rule affecting 32 CFR part 170 (published December 26, 2023, at 88 FR 89058) establishes that CMMC certification and CMMC self-assessments are required at the time of award.

14. Prime Contractor Validation of Subcontractor CMMC Level

Comment: Many respondents commented that there should be a way for prime contractors to validate subcontractor CMMC certificates and CMMC self-assessments.

Response: There is not currently a tool established that would allow sharing of subcontractor information with prime contractors electronically. Prime contractors are expected to work with their suppliers to conduct verifications as they would under any other clause requirement that applies to subcontractors.

15. Cost Allowability

Comment: Many respondents commented that the DFARS rule should specify whether costs for CMMC are allowable costs.

Response: Cost allowability requirements are described at FAR 31.201-2, Determining allowability.

16. Clause Applicability Overly Broad

Comment: Many respondents commented that the clause applicability is overly broad.

Response: In this proposed DFARS rule, the applicability of the clause has been narrowed to apply only when there is a requirement in the solicitation for the contractor to have a specific CMMC level.

17. Application to Plain Old Telephone Service (POTS)

Comment: One respondent asked if handling CUI under a POTS contract would trigger the requirements of DFARS 252.204-7012.

Response: 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). Common carrier telecommunications circuits or POTS would not normally be considered part of the covered contractor information system processing FCI or CUI. Data traversing common carrier systems should be separately encrypted per NIST SP 800-171 requirement 3.13.8. Contracts with common carriers to provide telecommunications services may include DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, but should not be interpreted to imply the common carrier telecommunications systems themselves have to meet the DFARS requirements.

18. Joint Ventures

Comment: Many respondents commented on how to handle CMMC certifications and CMMC self-assessments under joint ventures.

Response: Each individual entity that has a requirement for CMMC would be required to comply with the requirements related to the individual entity's information systems that process, store, or transmit FCI or CUI during contract performance.

19. Training on Marking CUI

Comment: Many respondents commented that DoD should train personnel on marking CUI and recommended that agencies do a better job of marking CUI.

Response: This comment is outside of the scope of this rule.

20. Clarification of How CMMC Applies to Information Systems

Comment: Many respondents commented that clarification is needed regarding how CMMC is applied to information systems.

Response: 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.

21. Fundamental Research

Comment: Many respondents commented that clarification is needed regarding whether CMMC applies to fundamental research.

Response: Fundamental research, as defined in National Security Decision Directive (NSDD) 189, is published and broadly shared within the scientific community and, as such, cannot be safeguarded as either FCI or CUI; however, if fundamental research has the potential to become CUI, it would be subject to the requirements of CMMC.

22. Clause Fill-in with CMMC Level

Comment: One respondent requested that the clause contain a fill-in with the CMMC level requirement.

Response: In this proposed rule, the CMMC level requirement will be included in the solicitation provision at 252.204-7YYY, Notice of Cybersecurity Model Certification Level Requirements and in the contract clause at 252.204-7021.

23. Application of CMMC to Non-COTS Item Contracts With No FCI or CUI Involved

Comment: Many respondents commented that it appears the CMMC clause would be included in non-COTS item contracts with no FCI or CUI involved at the prime contractor and subcontractor levels.

Response: The proposed rule prescribes the CMMC clause for use only in solicitations and contracts that require the contractor to have a specific CMMC level. Contracts that are exclusively for COTS items and purchases at or below the micro-purchase threshold will not have a requirement for the contractor to have a specific CMMC level.

24. Application of CMMC Clause to Service Contracts and Non-Defense Contracts

Comment: One respondent commented on whether the CMMC clause will be included in services contracts and non-defense contracts.

Response: The proposed rule proposes to amend the DFARS, so this proposed rule only includes changes to the requirements for DoD. A services contract may have a requirement for CMMC.

25. Definition of "contractor information system relevant to the contract/offer"

Comment: Many respondents requested clarification of the phrase, "contractor information system relevant to the contract/offer".

Response: The proposed rule includes language that clarifies that contractor information systems relevant to the contract or offer are contractor information systems that process, store, or transmit FCI or CUI during performance of the contract.

26. Effective Date of CMMC Clause for Contracts and Applicability to Modifications

Comment: Many respondents requested clarification on the effective date of the CMMC clause and applicability to modifications.

Response: The proposed rule includes amendments to the DFARS that will not take effect until a final rule is issued. Therefore, the effective date of the clause would be the effective date specified in the final rule. The clause will only be included in solicitations issued on or after the effective date of the final rule and any resulting contracts, unless the contracting officer makes a decision to include the clause in a solicitation issued prior to the effective date of the final rule, provided that any resulting contracts are awarded on or after the effective date of the final rule. Contracting officers have the discretion to bilaterally incorporate the clause in contracts in effect prior to the

effective date of the clause, with appropriate consideration. See FAR 1.108(d).

27. Determining CMMC Level for Subcontracts

Comment: Many respondents commented that there should be clarification regarding how to determine the required CMMC level for subcontracts.

Response: In determining a CMMC level appropriate for the information being flowed down to subcontractors, see the proposed rule affecting 32 CFR part 170 published in the **Federal Register** on December 26, 2023, at 88 FR 89058.

28. Proliferation of Component-unique Security Requirements

Comment: Many respondents commented that it appeared there was a proliferation of component-unique security requirements.

Response: While the comment is noted, the comment is outside of the scope of this proposed rule.

29. Reflecting CMMC Levels in SAM.gov for Prime Contractor Verification of Subcontractors

Comment: One respondent recommended reflecting CMMC levels in SAM.gov for prime contractor verification of the subcontractors.

Response: The CMMC Program proposed rule affecting 32 CFR part 170 has identified that SPRS is the repository for CMMC certificates and self-assessment information at present. Contractors will only be able to access their own CMMC certificate and self-assessment information.

30. Training Contracting Officers

Comment: Many respondents commented that it would be helpful to train contracting officers on how to appropriately identify contracts for inclusion of the DFARS clause at 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements.

Response: As with any clause, contracting officers will follow the prescription language in determining when to include a contract clause.

31. Vendor Description of CMMC Queue in Response to Proposals

Comment: One respondent commented recommending that an offeror should be able to share where they are in the queue for a CMMC assessment and be allowed to have a late submission of their CMMC certification.

Response: The CMMC Program policy, in the proposed rule affecting 32 CFR part 170, is to require a CMMC certification or CMMC self-assessment at the time of award if there is a requirement for CMMC under the contract.

32. Define "Certification"

Comment: A respondent commented that the term “certification” should be defined.

Response: The term ”certification” referenced in this proposed rule relates to the Cybersecurity Maturity Model Certification.

33. Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) Assessment Reciprocity

Comment: Several respondents asked for clarification on reciprocity between CMMC certification and Defense Contract Management Agency DIBCAC assessments.

Response: As described in the interim rule at DFARS 204.7501(c), the CMMC assessments will not duplicate efforts from any other comparable DoD assessment, except for rare circumstances when a reassessment may be necessary, for example, when there are indications of issues with cybersecurity and/or compliance with CMMC requirements.

34. Clearance Procedures for Interim Rule

Comment: A respondent asked what clearance procedures were bypassed to allow for the emergency processing of the previously published interim rule.

Response: Clearance procedures were not bypassed in the emergency processing of the previously published interim rule under this DFARS Case 2019-D041. As described in section IX of the preamble for the interim rule, a determination was made pursuant to 41 U.S.C. 1707(d) and FAR 1.501-3(b) to issue the interim rule.

35. Recommend Opening a DFARS Procedures, Guidance, and Information (PGI) Case

Comment: One respondent recommended that a PGI case should be opened to provide procedures, guidance, and information to the workforce related to CMMC.

Response: At present, the requirements in the proposed rule are simply for contracting officers to include the provision and

clause as prescribed. Any additional guidance would be for the program office and requiring activity community. Such guidance would not be added to the DFARS PGI, which speaks to contracting officers.

36. Existence of the Clause as an Indication of the Presence of CUI

Comment: Several respondents asked for clarification on whether the presence of the clause at 252.204-7021 means that CUI will be used in performance of the contract.

Response: CMMC also applies to FCI, so the existence of the clause at 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements, does not automatically mean that there is CUI that will be processed, stored, or transmitted in the performance of the contract.

37. Application of the Clause to Government Furnished Equipment (GFE)

Comment: One respondent requested clarification on whether the clause will apply to GFE or GFE in a test environment.

Response: If the program office or requiring activity includes a requirement in the solicitation and resulting contract for the contractor to have a specific CMMC level, then the clause would apply.

38. Other Contractual Instruments

Comment: A respondent commented that there should be a definition in the DFARS of "other contractual instruments".

Response: "Other contractual instruments" are agreements with vendors or suppliers that are not considered subcontracts. The term has been used in the DFARS for years and is well understood.

39. Source Selections

Comment: A respondent requested information on how CMMC applies to source selections.

Response: Proposed changes to DFARS 204.7503 require that contracting officers shall not award a contract, task order, or delivery order to an offeror that does not have a current CMMC certificate or self-assessment at the level required by the solicitation. If CMMC is included in a solicitation, it is also included as a contract requirement.

III. Applicability to Contracts at or Below the Simplified Acquisition Threshold (SAT), for Commercial Products (Including COTS Items), and for Commercial Services

This proposed rule amends the clause at DFARS 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements, as well as the prescription at DFARS 204.7504(a). The clause is prescribed for use in solicitations and contracts, task orders, or delivery orders, that require the contractor to have a specific CMMC level, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial products and commercial services, except for solicitations and contracts solely for the acquisition of COTS items. This proposed rule

includes a new provision, DFARS 252.204-7YYY, Notice of Cybersecurity Maturity Model Certification Level Requirements. The provision is prescribed at DFARS 204.7504(b) for use in solicitations that include the clause at DFARS 252.204-7021.

DoD intends to apply the provision and clause to contracts and subcontracts valued at or below the SAT but greater than the micro-purchase threshold, for the acquisition of commercial products excluding COTS items, and for the acquisition of commercial services.

A. Applicability to Contracts at or Below the Simplified Acquisition Threshold

41 U.S.C. 1905 governs the applicability of laws to contracts or subcontracts in amounts not greater than the simplified acquisition threshold. It is intended to limit the applicability of laws to such contracts or subcontracts. 41 U.S.C. 1905 provides that if a provision of law contains criminal or civil penalties, or if the Federal Acquisition Regulatory Council makes a written determination that it is not in the best interest of the Federal Government to exempt contracts or subcontracts at or below the SAT, the law will apply to them. The Principal Director, Defense Pricing, Contracting, and Acquisition Policy (DPCAP), is the appropriate authority to make comparable determinations for regulations to be published in the DFARS, which is part of the FAR system of regulations. DoD does intend to make that determination.

Therefore, this proposed rule will apply at or below the simplified acquisition threshold.

B. Applicability to Contracts for the Acquisition of Commercial Products Including COTS Items and for the Acquisition of Commercial Services

10 U.S.C. 3452 exempts contracts and subcontracts for the acquisition of commercial products including COTS items, and commercial services from provisions of law enacted after October 13, 1994, unless the Under Secretary of Defense (Acquisition and Sustainment) (USD(A&S)) makes a written determination that it would not be in the best interest of DoD to exempt contracts for the procurement of commercial products and commercial services from the applicability of the provision or contract requirement, except for a provision of law that—

- Provides for criminal or civil penalties;
- Requires that certain articles be bought from American sources pursuant to 10 U.S.C. 4862, or that strategic materials critical to national security be bought from American sources pursuant to 10 U.S.C. 4863; or
- Specifically refers to 10 U.S.C. 3452 and states that it shall apply to contracts and subcontracts for the acquisition of commercial products (including COTS items) and commercial services.

The statute implemented in this proposed rule does not impose criminal or civil penalties, does not require purchase pursuant to 10 U.S.C. 4862 or 4863, and does not refer to 10 U.S.C. 3452.

Therefore, section 1648 of the NDAA for FY 2020 will not apply to the acquisition of commercial services or commercial products including COTS items unless a written determination is made. Due to delegations of authority, the Principal Director, DPCAP is the appropriate authority to make this determination. DoD intends to make that determination to apply this statute to the acquisition of commercial products excluding COTS items and to the acquisition of commercial services. Therefore, this proposed rule will apply to the acquisition of commercial products excluding COTS items and to the acquisition of commercial services.

C. Determinations

Given that the requirements of section 1648 of the NDAA for FY 2020 were enacted to promote protection of FCI and CUI that will be processed, stored, or transmitted on contractor information systems, and since FCI and CUI may be processed, stored, or transmitted on contractor information systems in the performance of contracts or orders valued below the simplified acquisition threshold and when the Federal Government is procuring commercial products and commercial services, it is in the best interest of the Federal Government to apply the statute to contracts for the acquisition of commercial services and commercial products, excluding COTS items, as defined at FAR 2.101. An exception for contracts for the acquisition of commercial services and commercial products, excluding COTS items, would exclude the contracts intended to be covered by the

law, thereby undermining the overarching public policy purpose of the law.

IV. Expected Impact of the Rule

A. Background

DoD is proposing to amend the DFARS to implement the contractual requirements related to the DoD policy for CMMC 2.0 (see the proposed rule affecting 32 CFR 170, published in the **Federal Register** December 26, 2023, at 88 FR 89058). CMMC 2.0 self-assessments and certificates assess a contractor's compliance with certain information system security requirements. Pursuant to the DoD policy in the CMMC 2.0 proposed rule, the CMMC level requirements apply to every contractor information system that will process, store, or transmit Federal contract information (FCI) or controlled unclassified information (CUI).

DoD is proposing to amend the DFARS to include the following solicitation and contractual requirements related to the CMMC 2.0 policy:

- Offeror and contractor requirement to post the results of a CMMC 2.0 Level 1 or Level 2 self-assessment to the Supplier Performance Risk System (SPRS) prior to award, exercise of an option, or extension of a period of performance, if not already posted.
- Contractor requirement to maintain the required CMMC self-assessment or certificate level for the life of the contract.

- Contractor requirement to complete a contractor senior company official affirmation of continuous compliance with the security requirements identified at 32 CFR part 170 in SPRS for each DoD unique identifier (UID) applicable to each of the contractor information systems that will process, store, or transmit FCI or CUI and that will be used in performance of the contract on an annual basis, or when CMMC 2.0 compliance status changes occur.
- Apparently successful offeror and contractor requirement to identify the contractor information systems that will be used to process, store, or transmit FCI or CUI in performance of the contract prior to award, exercise of an option, or extension of any period of performance, by providing to the Government the DoD UIDs generated by SPRS.

The costs associated with the technical completion of the CMMC 2.0 certifications and self-assessments are included in the CMMC 2.0 proposed rule affecting title 32 CFR.

B. Summary of Impact

This proposed DFARS rule will impact certain contracts during a phased-in, three-year implementation period. Afterwards, the requirements will apply to all contracts for which the contractor will process, store, or transmit FCI or CUI on contractor information systems during the performance of the contract, except for contracts solely for the acquisition of commercially available off-the-shelf (COTS) items.

For the first three years after the effective date of the final rule, the information collection requirements will only impact an offeror or contractor when the solicitation or contract requires an offeror or contractor to have a specific CMMC level, based on a phased rollout plan, including solicitations and contracts using Federal Acquisition Regulation (FAR) part 12 procedures for the acquisition of commercial products and commercial services, except for solicitations and contracts solely for the acquisition of COTS items.

By the fourth year, the information collection requirements in the solicitation provision and contract clause will impact solicitations and contracts, task orders, or delivery orders, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial products and commercial services, when there will be a requirement under the contract to process, store, or transmit FCI or CUI, except for solicitations and contracts solely for the acquisition of COTS items.

Since DoD does not track awards that may include FCI or CUI, DoD assumes the number of impacted awardees in Year 4 and beyond will be the average number of entities in the Electronic Data Access (EDA) system from fiscal year (FY) 2021 through FY 2023 with awards containing the clause at DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, or 29,543 entities, of which 20,395 (69 percent) are small businesses. DoD also assumes that offerors or contractors

with a requirement for CMMC in contracts will have on average 5 contractor information systems that will be used to process, store, or transmit FCI or CUI in performance of the contract.

For each of the information systems that will process, store, or transmit FCI or CUI, DoD assumes it will take offerors and contractors—

- An estimated 5 minutes to post the results of the CMMC self-assessments in SPRS;
- An estimated 5 minutes to complete the required affirmation in SPRS; and
- An estimated 5 minutes to retrieve DoD UIDs in SPRS for the information systems that will be used in performance of the contract and to submit the DoD UIDs to the Government.

For the Government, DoD assumes it will take—

- An estimated 5 minutes to validate the existence of the correct level and currency of a CMMC certification or CMMC self-assessment results associated with offeror DoD UIDs in SPRS for the apparently successful offeror prior to award and for the contractor prior to exercising an option or extending any period of performance;
- An estimated 5 minutes to validate the existence of an affirmation that is current for each of the contractor information systems that will process, store, or transmit FCI or CUI; and
- An estimated 5 minutes to validate the existence of the correct level and currency of a CMMC certification or CMMC

self-assessment and affirmation associated with contractor DoD UIDs in SPRS, when there are changes in the information systems during contract performance.

The primary cost impact of this proposed rule is that apparently successful offerors for contracts that include a CMMC requirement will now be required to conduct the cost activities described below in accordance with the provision at DFARS 252.204-7YYY, Notice of Cybersecurity Maturity Model Certification Level Requirement, and the clause at DFARS 252.204-7021, Cybersecurity Maturity Model Certification Requirements.

The benefits of this proposed rule include verification of a defense industrial base (DIB) contractor's implementation of system security requirements. The clause at DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, does not provide for the DoD verification of a DIB contractor's implementation of the security requirements specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 prior to contract award. CMMC adds the element of verification of a DIB contractor's cybersecurity through the use of accredited third-party assessors. This proposed rule provides increased assurance to DoD that a DIB contractor can adequately protect sensitive unclassified information such as CUI at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain.

Another benefit of this proposed rule is that it supports the protection of intellectual property and sensitive information from malicious activity that has a significant impact on the U.S. economy and national security. While there is not enough information to be able to estimate the benefits of this rule at this time, DoD assumes there will be a benefit from reducing the threat of malicious cyber activity. The Council of Economic Advisors estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016. Over a ten-year period, that burden would equate to an estimated $512 billion to $979 billion in costs at a 2 percent discount rate.

The following is a summary of the estimated public and Government costs calculated over a 10-year period at a 2 percent discount rate:

SUMMARY	Public	Government	Total
Present Value	$40,687,957	$25,237,882	$65,925,839
Annualized Costs	$4,529,649	$2,809,646	$7,339,295

Public comments are solicited on this analysis of the estimated burden of the proposed rule.

V. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select

regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This is a significant regulatory action and, therefore, was subject to review under section 6(b) of E.O. 12866, Regulatory Planning and Review, as amended.

VI. Regulatory Flexibility Act

DoD does not expect this proposed rule, when finalized, to have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601, *et seq*. However, an initial regulatory flexibility analysis has been performed and is summarized as follows:

This proposed rule is necessary to respond to the threat to the U.S. economy and national security posed by ongoing malicious cyber activities designed to steal hundreds of billions of dollars of U.S. intellectual property. This proposed rule includes the following requirements for apparently successful offerors responding to a solicitation, and contractors awarded contracts, containing a requirement for CMMC: (1) post in SPRS the results of a current CMMC certificate or current CMMC self-assessment at the level required by the solicitation, or higher, for each DoD UID applicable to each of the contractor information systems that will process, store, or

transmit FCI or CUI and that will be used in performance of the contract and maintain the CMMC level for the life of the contract; (2) provide the DoD UID(s) applicable to each of those contractor information systems to the contracting officer and provide updates, if applicable; and (3) have a current affirmation of continuous compliance with the security requirements identified at 32 CFR part 170 in SPRS for each DoD UID applicable to each of those contractor information systems. These requirements apply to apparently successful offerors with a CMMC requirement in solicitations prior to award and to contractors with a CMMC requirement in contracts prior to exercising an option.

The proposed rule has two objectives. One objective is to provide DoD with assurances that a defense industrial base contractor can adequately protect sensitive unclassified information at a level commensurate with the risk, accounting for information shared with its subcontractors in a multi-tier supply chain. Another objective is to partially implement section 1648 of the NDAA for FY 2020. The legal basis for the rule is 41 U.S.C. 1303 and section 1648 of the NDAA for FY 2020.

Given the enterprise-wide implementation of CMMC, DoD developed a three-year phased rollout strategy. The rollout is intended to minimize both the financial impacts to the industrial base, especially small entities, and disruption to the existing DoD supply chain. Upon completion of the phased implementation, this rule will impact all small entities awarded

contracts with DoD, except those providing only COTS items and those that do not handle FCI or CUI. The estimated number of small entities to which the rule will apply in year one is 1,104.

By the fourth year, all entities receiving DoD contracts and orders that have contractor information systems that will process, store, or transmit FCI or CUI and that will be used in performance of the contract or order, other than contracts or orders exclusively for COTS items, will be required to have, at minimum, a CMMC Level 1 self-assessment or the CMMC Level identified in the solicitation and resulting contract, as appropriate for the type of information being handled under the contract. As described previously, it should be noted that this requirement does not apply to awards that do not involve the handling or transmission of FCI or CUI. By year four, the total estimated number of small entities to which the rule will apply will be 60,783.

During the first three years of the phased rollout, the CMMC requirement will be included only in certain contracts for which the CMMC Program Office directs DoD component program offices to include a CMMC requirement. After three years, DoD component program offices will be required to include a requirement for CMMC in solicitations and contracts that will require the contractor to process, store, or transmit FCI or CUI on contractor information systems during contract performance. Not every contractor will be awarded a contract in Year 4, so it

will take several years for every contractor in the defense industrial base to be awarded a contract containing a requirement for CMMC. DoD does not track how many years it takes for every contractor to be awarded a DoD contract, so DoD assumes this will occur over a period of several years.

Based on data from the Electronic Data Access system for FY 2021 through FY 2023, the number of unique entities with contracts containing the clause at DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, is 29,543, of which 20,395 (69 percent) are small entities. Therefore, DoD estimates that in Year 4 and beyond, approximately 20,395 small entities will be impacted per year. DoD anticipates that the following mix of self-assessments and certificates will occur starting in Year 4; however, it is likely to change based on component program office discretion regarding whether a CMMC self-assessment or certificate is required and, if so, at what level:

CMMC Level	Percentages	Small Entities	Large Entities	Total Entities
Level 1 Self-assessment	63%	12,849	5,763	18,612
Level 2 Self-assessment	2%	408	183	591
Level 2 Certificate	35%	7,138	3,202	10,340
Total Entities	100%	20,395	9,148	29,543

This proposed rule includes new reporting, recordkeeping, or other compliance requirements for small entities. The following

is a summary of the projected reporting and other compliance requirements associated with the proposed rule: (1) a requirement for apparently successful offerors to post results of current CMMC Level 1 and Level 2 self-assessments to SPRS for each DoD UID applicable to each of the contractor information systems that will process, store, or transmit FCI or CUI and that will be used in performance of the contract, if applicable; (2) a requirement for apparently successful offerors and contractors to provide DoD UIDs for each of those contractor information systems, if applicable, prior to award and when any changes to DoD UIDs occur; and (3) a requirement for a senior company official to complete and maintain on an annual basis, or when CMMC compliance status changes occur, the affirmation of continuous compliance with the security requirements identified at 32 CFR part 170 in SPRS for each DoD UID applicable to each of those contractor information systems.

These reporting requirements would apply to any small entities that are the apparently successful offeror for a contract for which there is a requirement for a specific CMMC level. The requirement to post the self-assessment will only apply to small entities that have a requirement for a CMMC Level 1 or Level 2 self-assessment. The requirement to provide DoD UIDs and the requirement for the senior official to complete the affirmation in SPRS will apply to all small entities that are apparently successful offerors for a solicitation or contractors awarded a contract for which there is a requirement for CMMC.

This proposed rule does not duplicate, overlap, or conflict with any other Federal rules. This proposed DFARS rule implements the contractual requirements related to the CMMC 2.0 program, which was published as a separate proposed rule affecting 32 CFR part 170 on December 26, 2023, at 88 FR 89058.

There are no known alternatives that would accomplish the stated objectives of the applicable statute. This proposed rule uses a phased rollout approach to implementation and applies the CMMC requirements only to apparently successful offerors for solicitations and contractors awarded a contract containing a CMMC requirement. This proposed rule exempts contracts and orders exclusively for the acquisition of COTS items to minimize any significant economic impact of the proposed rule on small entities. Because of the across-the-board risks of not implementing cybersecurity requirements, DoD was unable to identify any additional alternatives that would reduce the burden on small entities and still meet the objectives of the proposed rule.

DoD invites comments from small business concerns and other interested parties on the expected impact of this proposed rule on small entities.

DoD will also consider comments from small entities concerning the existing regulations in subparts affected by this proposed rule in accordance with 5 U.S.C. 610. Interested parties must submit such comments separately and should cite 5 U.S.C. 610 (DFARS Case 2019-D041), in correspondence.

VII. Paperwork Reduction Act

This proposed rule contains information collection requirements that require the approval of the Office of Management and Budget under the Paperwork Reduction Act (44 U.S.C. chapter 35). Accordingly, DoD has submitted a request for approval of a new information collection requirement concerning 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements, to the Office of Management and Budget.

A. Estimate of Public Burden

Public reporting burden for this collection of information is estimated to average 5 minutes (0.8333) per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information.

The annual reporting burden is estimated as follows:

Respondents: 1,493.

Total annual responses: 30,990.

Total annual burden hours: 2,582.

B. Request for Comments Regarding Paperwork Burden

Written comments and recommendations on the proposed information collection, including suggestions for reducing this burden, should be submitted using the Federal eRulemaking Portal at *https://www.regulations.gov* or by email to *osd.dfars@mail.mil*. Comments can be received up to 60 days after the date of this notice.

Public comments are particularly invited on: whether this collection of information is necessary for the proper performance of the functions of DoD, including whether the information will have practical utility; the accuracy of DoD's estimate of the burden of this information collection; ways to enhance the quality, utility, and clarity of the information to be collected; and ways to minimize the burden of the information collection on respondents, including through the use of automated collection techniques or other forms of information technology.

To obtain a copy of the supporting statement and associated collection instruments, please email *osd.dfars@mail.mil*. Include DFARS Case 2019-D041 in the subject line of the message.

List of Subjects in 48 CFR Parts 204, 212, 217, and 252

Government procurement.

Jennifer D. Johnson,

Editor/Publisher, Defense Acquisition Regulations System.

Therefore, the Defense Acquisition Regulations System proposes to amend 48 CFR parts 204, 212, 217, and 252 as follows:

1. The authority citation for 48 CFR parts 204, 212, 217, and 252 continues to read as follows:

Authority: 41 U.S.C. 1303 and 48 CFR chapter 1.

PART 204—ADMINISTRATIVE AND INFORMATION MATTERS

2. Revise subpart 204.75 to read as follows:

Subpart 204.75—Cybersecurity Maturity Model Certification

Sec.

204.7500 Scope of subpart.

204.7501 Definitions.

204.7502 Policy.

204.7503 Procedures.

204.7504 Solicitation provision and contract clause.

Subpart 204.75—Cybersecurity Maturity Model Certification

204.7500 Scope of subpart.

(a) This subpart prescribes policies and procedures for including the Cybersecurity Maturity Model Certification (CMMC) level requirements in DoD contracts. CMMC is a framework (see 32 CFR part 170) for assessing a contractor's compliance with applicable information security requirements (see *https://DoDcio.defense.gov/CMMC/*).

(b) This subpart does not abrogate any other requirements regarding contractor physical, personnel, information, technical, or general administrative security operations governing the protection of unclassified information, nor does it affect requirements of the National Industrial Security Program.

204.7501 Definitions.

As used in this subpart—

Controlled unclassified information means information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Governmentwide policy requires or permits an

agency to handle using safeguarding or dissemination controls (32 CFR 2002.4(h)).

Current means, with regard to Cybersecurity Maturity Model Certification—

(1) Not older than 1 year for Level 1 self-assessments, with no changes in CMMC compliance since the date of the assessment;

(2) Not older than 3 years for Level 2 certificates and self-assessments, with no changes in CMMC compliance since the date of the assessment;

(3) Not older than 3 years for Level 3 certificates, with no changes in CMMC compliance since the date of the assessment; and

(4) Not older than 1 year for affirmations of continuous compliance with the security requirements identified at 32 CFR part 170, with no changes in CMMC compliance since the date of the affirmation.

DoD unique identifier means an alpha-numeric string of ten characters assigned within the Supplier Performance Risk System to each contractor assessment with the first two characters indicating the confidence level of the assessment.

204.7502 Policy.

(a) The CMMC certificate or CMMC self-assessment level specified in the contract is required for all information systems, used in the performance of the contract, that will

process, store, or transmit Federal contract information (FCI) or controlled unclassified information (CUI).

(b) Contractors are required to achieve, at time of award, a CMMC certificate or CMMC self-assessment at the level specified in the solicitation, or higher. Contractors 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.

(c) The CMMC assessments shall not duplicate efforts from any other comparable DoD assessment, except for rare circumstances when a re-assessment may be necessary, for example, when there are indications of issues with cybersecurity and/or compliance with CMMC requirements.

204.7503 Procedures.

(a) The contracting officer shall include the CMMC level required by the program office or requiring activity in the solicitation and contract.

(b)(1) Contracting officers shall not award a contract, task order, or delivery order to an offeror that does not have—

(i) The results of a current CMMC certificate or current CMMC self-assessment at the level required by the solicitation, or higher, for each DoD unique identifier (DoD UID) applicable to each of the contractor information systems that will process, store, or transmit FCI or CUI and that will be used in

performance of the contract posted in the Supplier Performance Risk System (SPRS) (see 32 CFR 170.15 through 170.18); and

(ii) A current affirmation of continuous compliance with the security requirements identified at 32 CFR part 170 in SPRS for each DoD UID applicable to each of the contractor information systems that will process, store, or transmit FCI or CUI and that will be used in performance of the contract.

(2) Contracting officers shall require the apparently successful offeror to provide the DoD UID(s) applicable to each of the contractor information systems that will process, store, or transmit FCI or CUI and that will be used in performance of the contract. The contracting officer shall ensure the program office or requiring activity reviews the information described in paragraphs (b)(1)(i) and (ii) of this section.

(c)(1) Contracting officers shall not exercise an option period or extend the period of performance on a contract, task order, or delivery order, unless the contractor has—

(i) A current CMMC certificate or CMMC self-assessment at the level required by the contract, task order, or delivery order, or higher, for each DoD UID applicable to each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract; and

(ii) A current affirmation of continuous compliance with the security requirements identified at 32 CFR part 170 in SPRS for each DoD UID applicable to each of the contractor information systems that process, store, or transmit FCI or CUI

and that are used in performance of the contract (see 252.204-7021, paragraph (b)(5)).

(2) The contracting officer shall ensure the program office or requiring activity reviews the information described in paragraphs (c)(1)(i) and (ii).

(d) If the contractor provides new DoD UIDs during performance of the contract, the contracting officer shall ensure the program office or requiring activity verifies in SPRS that the contractor—

(1) Has a current affirmation of continuous compliance with the security requirements identified at 32 CFR part 170 for each DoD UID applicable to each of the contractor information systems that process, store, or transmit FCI or CUI (see 252.204-7021, paragraph (b)(5)); and

(2) Has a current CMMC certificate or CMMC self-assessment at the required level, or higher, for each information system identified that will process, store, or transmit FCI or CUI during contract performance using the DoD UIDs assigned by SPRS.

204.7504 Solicitation provision and contract clause.

(a) Use the clause at 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements, in solicitations and contracts, task orders, or delivery orders that require the contractor to have a CMMC certificate or CMMC self-assessment at a specific level, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, except for

solicitations and contracts or orders solely for the acquisition of commercially available off-the-shelf items.

(b) Use the provision at 252.204-7YYY, Notice of Cybersecurity Maturity Model Certification Level Requirements, in solicitations that include the clause at 252.204-7021.

PART 212—ACQUISITION OF COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

3. Amend section 212.301—

a. In paragraph (f)(ii)(L) by removing "204.7503(a) and (b)" and adding "204.7504(a)" in its place; and

b. By adding paragraph (f)(ii)(P) to read as follows:

212.301 Solicitation provisions and contract clauses for the acquisition of commercial products and commercial services.

* * * * *

(f) * * *

(ii) * * *

(P) Use the provision at 252.204-7YYY, Notice of Cybersecurity Maturity Model Certification Level Requirements, as prescribed in 204.7504(b).

* * * * *

PART 217—SPECIAL CONTRACTING METHODS

4. Amend section 217.207—

a. In paragraph (c) introductory text by removing "after:" and adding "after—" in its place;

b. In paragraph (c)(1) by removing the period at the end of the paragraph and adding "; and" in its place;

c. By revising paragraph (c)(2) introductory text;

d. In paragraph (c)(2)(i) by removing the period at the end of the paragraph and adding "; and" in its place; and

e. By revising paragraph (c)(2)(ii).

The revisions read as follows:

217.207 Exercise of options.

(c) * * *

(2) Ensuring the program office or requiring activity verifies in the Supplier Performance Risk System (*https://piee.eb.mil*) that—

* * * * *

(ii) If there is a requirement for the contractor to have a Cybersecurity Maturity Model Certification (CMMC) certificate or CMMC self-assessment at a specific level, the contractor has the required affirmation(s) of continuous compliance with the security requirements identified at 32 CFR part 170 and has posted the results of a current (see 204.7501) CMMC certificate or CMMC self-assessment at the level required by the contract, or higher. See 204.7503(c).

PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

5. Revise section 252.204-7021 to read as follows:

252.204-7021 Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements.

As prescribed in 204.7504(a), insert the following clause:

CONTRACTOR COMPLIANCE WITH THE CYBERSECURITY MATURITY MODEL CERTIFICATION LEVEL REQUIREMENTS (DATE)

(a) *Definitions*. As used in this clause–

Controlled unclassified information means information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls (32 CFR part 2002.4(h)).

Current means, with regard to Cybersecurity Maturity Model Certification (CMMC)—

(1) Not older than 1 year for Level 1 self-assessments, with no changes in CMMC compliance since the date of the assessment;

(2) Not older than 3 years for Level 2 certificates and self-assessments, with no changes in CMMC compliance since the date of the assessment;

(3) Not older than 3 years for Level 3 certificates, with no changes in CMMC compliance since the date of the assessment; and

(4) Not older than 1 year for affirmations of continuous compliance with the security requirements identified at 32 CFR part 170, with no changes in CMMC compliance since the date of the affirmation.

Cybersecurity Maturity Model Certification means a framework for assessing a contractor’s compliance with applicable information security requirements (see 32 CFR part 170).

DoD unique identifier means an alpha-numeric string of ten characters assigned within the Supplier Performance Risk System to each contractor assessment, with the first two characters indicating the confidence level of the assessment.

(b) *Requirements*. The Contractor shall—

(1)(i) Have a current CMMC certificate or current CMMC self-assessment at the following CMMC level, or higher: _____ *[Contracting Officer to fill in the required CMMC level]*; and

(ii) Consult 32 CFR part 170 related to flowing down information in order to establish the correct CMMC level requirements for subcontracts and other contractual instruments;

(2) Maintain the CMMC level required by this contract for the duration of the contract for all information systems, used in performance of the contract, that process, store, or transmit Federal contract information (FCI) or controlled unclassified information (CUI);

(3) Only process, store, or transmit data on information systems that have a CMMC certificate or CMMC self-assessment at the CMMC level required by the contract, or higher;

(4) Notify the Contracting Officer within 72 hours when there are any lapses in information security or changes in the status of CMMC certificate or CMMC self-assessment levels during performance of the contract;

(5) Complete and maintain on an annual basis, or when changes occur in CMMC compliance status (see 32 CFR part 170),

an affirmation of continuous compliance with the security requirements associated with the CMMC level required in paragraph (b)(1) of this clause in the Supplier Performance Risk System (SPRS) (*https://piee.eb.mil*) for each DoD unique identifier (DoD UID) applicable to each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract; and

(6) Ensure all subcontractors and suppliers complete and maintain on an annual basis, or when changes occur in CMMC compliance status (see 32 CFR part 170), an affirmation of continuous compliance with the security requirements associated with the CMMC level required for the subcontract or other contractual instrument for each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract.

(c) *Reporting*. The Contractor shall—

(1) Submit to the Contracting Officer the DoD UID(s) issued by SPRS for contractor information systems that will process, store, or transmit FCI or CUI during performance of the contract;

(2) Enter into SPRS the results of self-assessment(s) for each DoD UID applicable to each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract; and

(3) Report to the Contracting Officer any changes to the list of DoD UIDs applicable to each of the contractor

information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract.

(d) *Subcontracts*. The Contractor shall—

(1) Insert the substance of this clause, including this paragraph (d), and exclude paragraphs (b)(5) and (c), in subcontracts and other contractual instruments, including those for the acquisition of commercial products and commercial services, excluding commercially available off-the-shelf items, when there is a requirement under the subcontract or similar contractual instrument for a CMMC level; and

(2) Prior to awarding a subcontract or other contractual instrument, ensure that the subcontractor has a current CMMC certificate or current CMMC self-assessment at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor.

(End of clause)

6. Add section 252.204-7YYY to read as follows:

252.204-7YYY Notice of Cybersecurity Maturity Model Certification Level Requirements.

As prescribed in 204.7504(b) use the following provision:

NOTICE OF CYBERSECURITY MATURITY MODEL CERTIFICATION LEVEL REQUIREMENTS (DATE)

(a) *Definitions*. As used in this provision, *controlled unclassified information*, *current*, *Cybersecurity Maturity Model Certification*, and *DoD unique identifier* have the meaning given in the Defense Federal Acquisition Regulation Supplement

252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements, clause of this solicitation.

(b)(1) *Cybersecurity Maturity Model Certification (CMMC) level*. The CMMC certificate or CMMC self-assessment level required by this solicitation is: _____ *[Contracting Officer insert: CMMC Level 1 self-assessment; CMMC Level 2 certificate or CMMC self-assessment; or CMMC Level 3 certificate]*. This CMMC certificate or CMMC self-assessment level, or higher, is required prior to award for each contractor information system that will process, store, or transmit Federal contract information (FCI) or controlled unclassified information (CUI) during performance of the contract.

(2) The apparently successful offeror will not be eligible for award of a contract, task order, or delivery order resulting from this solicitation if the apparently successful offeror does not have the results of a current CMMC certificate or self-assessment entered in the Supplier Performance Risk System (SPRS) (*https://piee.eb.mil*) at the CMMC level required by paragraph (b)(1) of this provision and an affirmation of continuous compliance with the security requirements identified at 32 CFR part 170 in SPRS for each of the contractor information systems that will process, store, or transmit FCI or CUI and that will be used in performance of a contract resulting from this solicitation.

(c) *DoD unique identifiers.* At the request of the Contracting Officer, the apparently successful offeror shall provide the DoD unique identifier(s) issued by SPRS for each contractor information system that will process, store, or transmit FCI or CUI during performance of a contract, task order, or delivery order resulting from this solicitation. The DoD unique identifier(s) are provided in SPRS after the Offeror enters the results of self-assessment(s) for each such information system.

(End of provision)

[FR Doc. 2024-18110 Filed: 8/14/2024 8:45 am; Publication Date: 8/15/2024]