5001-FR-P

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: Final rule.

SUMMARY: DoD is issuing a final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to incorporate contractual requirements related to the final Cybersecurity Maturity Model Certification program rule, titled Cybersecurity Maturity Model Certification Program. This final 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: This rule is effective **[INSERT DATE 60 DAYS FROM DATE OF PUBLICATION IN THE FEDERAL REGISTER].**

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

SUPPLEMENTARY INFORMATION:

I. Background

DoD published an interim rule in the **Federal Register** at 85 FR 61505 on September 29, 2020, to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain. DoD subsequently published a proposed rule in the **Federal Register** at 89 FR 66327 on August 15, 2024, to implement the contractual requirements related to the Cybersecurity Maturity Model Certification (CMMC) program. Ninety-seven respondents submitted public comments in response to the proposed rule.

Separately, a proposed rule to establish the CMMC program at 32 CFR part 170, Cybersecurity Maturity Model Certification Program, was published in the **Federal Register** at 88 FR 89058 on December 26, 2023. A final rule was published in the **Federal Register** at 89 FR 83092 on October 15, 2024, and became effective on December 16, 2024.

II. Discussion and Analysis

DoD reviewed the public comments in the development of the final rule. A discussion of the comments and the changes made to the rule as a result of those comments is provided, as follows:

A. Summary of Significant Changes From the Proposed Rule

The following significant changes from the proposed rule are made in the final rule:

1. Definitions

The final rule adds and modifies certain definitions at DFARS 204.7501, Definitions. The definition of "current" was changed to clarify that it is related to having no changes in compliance with the requirements at 32 CFR part 170. The definition of "current" was also updated to clarify what "current" means when referring to "Conditional CMMC Status", "Final CMMC Status", and "affirmation of continuous compliance." The term "DoD unique identifier" was updated to "CMMC unique identifier" to match the naming convention in the Supplier Performance Risk System (SPRS). The definition of CMMC unique identifier (UID) clarifies that it means ten alpha-numeric characters assigned to each contractor CMMC assessment and reflected in SPRS for each contractor information system.

The final rule adds the definition of "Federal contract information" based on the definition from the clause at Federal Acquisition Regulation (FAR) 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, to provide clarity as the term is used widely throughout the rule. The final rule adds a definition of "plan of action and milestones" (POA&M) based on the definition codified at 32 CFR part 170, given this term has been added to the rule. The final rule also adds the term "CMMC status" and a definition for the term to clarify for contracting officers what they will view in SPRS when performing reviews of an offeror or contractor's CMMC status.

2. Policy

DFARS 204.7502, Policy, includes language to add more clarity by stating that for CMMC levels 2 and 3 only, a conditional CMMC status is permitted for a period not to exceed 180 days from the conditional CMMC date, in accordance with 32 CFR 170.21, and an award can occur with a CMMC conditional status. The language at DFARS 204.7502 has also been updated to include a statement that a final CMMC is achieved upon successful closeout of a valid POA&M, which clarifies the policy related to POA&Ms.

3. Procedures

The language at DFARS 204.7503 was updated to add paragraph headings to clarify the topic addressed in each paragraph. Language was updated to clarify that contracting officers are required to check SPRS and not award a contract, task order, or delivery order to an offeror that does not have a current CMMC status posted in SPRS at the CMMC level required by the solicitation, or higher, for each CMMC UID provided by the offeror applicable to each of the contractor information systems that will process, store, or transmit FCI or CUI and be used in performance of the contract posted in SPRS. The language at paragraph (d) has been updated to clarify that all offerors are required to provide the CMMC UIDs applicable to each of the contractor information systems that process, store, or transmit FCI or CUI and that will be used in performance of the contract.

4. Clause Prescription

At DFARS 204.7504 the prescription for the contract clause has been updated to clarify the phased implementation approach based

on public comments that indicated some uncertainty with the timeline. The prescription was updated to clarify that, unless the requirements at 32 CFR 170.5(d) are met, until three years after the effective date of the rule, the clause will be prescribed for use if program managers and requiring activities make a determination to apply a CMMC requirement to contracts, excluding awards solely for the acquisition of commercially available off-the-shelf (COTS) items. Beginning three years and one day after the effective date of the rule, the clause will be prescribed for use if program managers and requiring activities determine that the contractor will be required to use contractor information systems in the performance of the contract, task order, or delivery order to process, store, or transmit FCI or CUI, excluding awards solely for the acquisition of COTS items.

5. Solicitation Provision and Contract Clause

The contract clause has been updated to include a fill-in for the contracting officer to identify the CMMC level required by the contract. The subcontract flowdown language in the clause has been updated to identify that subcontractors also must submit affirmations of continuous compliance and the results of self-assessments in SPRS. The clause has been updated to include the term "affirming official" in place of "senior company official" to match the language codified at 32 CFR part 170.

The solicitation provision and contract clause have been updated to include the terminology the contracting officer will

need to use when entering the CMMC level required by the solicitation and contract, which includes: CMMC Level 1 (Self); CMMC Level 2 (Self); CMMC Level 2 (C3PAO); or CMMC Level 3 (DIBCAC).

The solicitation provision was updated to clarify that offerors will not be eligible for award of a contract, task order, or delivery order resulting from a solicitation containing the provision, if the offeror does not have the results of a current CMMC status entered in SPRS at the CMMC level required by paragraph (b)(1) of the provision and a current 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 be used in performance of an award resulting from the solicitation. The solicitation provision was also updated to clarify that all offerors will be required to provide, with the proposal, the CMMC UIDs 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 a solicitation containing the provision. Offerors will also be required to update the list when new CMMC UIDs are provided in SPRS.

B. Analysis of Public Comments

Technical and programmatic comments on CMMC were addressed in the CMMC program rule that codified the CMMC program requirements at 32 CFR part 170. In addition, the comments

related to the CMMC cost analysis were also addressed under the CMMC program rule that codified 32 CFR part 170. This DFARS rule addresses the nontechnical and nonprogrammatic comments.

1. Clarification of "Changes"

Comment: Several respondents asked for more clarity regarding what "changes" means in the proposed rule. A respondent recommended changing paragraph (c)(3) of the clause at 252.204-7021 to "Report to the Contracting Officer any changes to the information reported in SPRS for the list of CMMC 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" instead of "Report to the Contracting Officer any changes to the list of CMMC 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."

Response: Based on the public comment, and to add clarity, the final DFARS rule has added the sentence, "Submit to the Contracting Officer ... any changes in the CMMC UIDs generated in SPRS throughout the life of the contract, task order, or delivery order, if applicable." This new sentence takes the place of the sentence, "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."

Comment: A respondent recommended that the CMMC notification requirement for lapses in information security or CMMC certification should be removed and instead recommended that CMMC certification status changes be managed via the Cyber Accreditation Board and the CMMC accreditation and certification process. A couple of respondents recommended removing the contracting officer notification requirement and relying upon the DIBNET portal notification and use of SPRS for monitoring supplier compliance. Another respondent stated that there should not be a requirement for contractors to report "any changes" in contractor information systems. Several respondents stated that the 72-hour reporting requirement at DFARS 252.204-7012 paragraph (c) provides sufficient notification of relevant information security incidents.

Response: Based on public comments, the notification requirement in this rule to report to the contracting officer lapses in information security or changes in compliance with 32 CFR part 170 was removed. The reporting requirement at DFARS 252.204-7012 paragraph (c) to provide notification of information security incidents and the annual affirmation of continuing compliance will offer ongoing protection for DoD information.

Comment: Several respondents stated that the rule should clarify which changes are acceptable and which would void a contractor's CMMC certification. A few respondents stated that a threshold for changes should be included. Other respondents

stated that guidance and definitions on changes should be included. Several respondents requested a clarification on what "security changes" mean in the context of the proposed rule clause. A respondent stated the notification requirements under the rule should be aligned with a forthcoming Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) rule. Another respondent recommended focusing the incident reporting requirements under DFARS 252.204-7021 paragraph (b)(4) solely on reporting changes in the status of the CMMC certificate levels or CMMC self-assessment levels during performance of the contract. A respondent stated that including subcontractors within the scope of reporting is unnecessary and duplicates other mandated reporting requirements.

Response: Based on public comments, the final rule removes the requirement to report lapses in information security or changes in compliance with 32 CFR part 170 to the contracting officer. The reporting requirement at DFARS 252.204-7012 paragraph (c) provides sufficient notification of information security incidents. Therefore, an additional reporting requirement in this rule is not necessary to protect DoD information.

2. Clarification of "Lapses in Information Security"

Comment: Several respondents asked for more clarity regarding what "lapses in information security" means in the proposed clause language in paragraph (b)(4) at DFARS 252.204-7021. Another respondent requested clarity regarding notifications and

responses related to "lapses in information security." Several respondents stated that "lapses in information security" should be removed from the rule.

Response: Based on public comments, the requirement to notify the contracting officer of lapses in information security or changes in the status of CMMC certificate or CMMC self-assessment levels during performance of the contract has been removed from the final rule.

3. Editorial Changes

Comment: A respondent mentioned that there were typos in the Federal Register notice and stated that 205.7502 should be "Procedures", 204.7503 should be "Contract Clause", and 205.7501 should be "Policy." Another respondent mentioned that there appeared to be a missing word in paragraph (b)(4) of the clause and recommended changing the sentence to, "Notify the Contracting Officer within 72 hours when there are any lapses in information security or changes in the status of CMMC certificate or changes in the status of CMMC self-assessment levels during performance of the contract." A few respondents recommended using "and/or" instead of "or" when referring to the CMMC UIDs that will be issued by SPRS when FCI or CUI is being processed, stored, or transmitted.

Response: While the editorial comments have been noted, changes have been made in the final rule that result in these comments no longer being applicable, with the exception of the comment to include "and/or" in place of "or" in the final rule.

The recommendation to include "and/or" in the final rule was not implemented, because it may narrow the scope of the requirement beyond what was intended.

4. CMMC Level Notification and Compliance

Comment: A couple of respondents commented that it was unclear how they will be notified of the required CMMC level for the information system or information systems that will be used in performance of the contract that process, store, or transmit FCI or CUI and how that level will be determined. A respondent stated that it was their assumption that CMMC only has the Level 2 certification or Level 2 self-assessment. Another respondent recommended DoD limit inclusion of CMMC in existing contracts unless the risk warrants inclusion. A respondent (asked whether contracting officers can take feedback from bidders on whether the CMMC level is correct and whether there will be an exemption for small businesses during the phase-in period. The respondent requested feedback on whether there will be exemptions for an in-process C3PAO assessment.

Response: The CMMC level determination is made in accordance with 32 CFR part 170 by the program office or requiring activity for the prime contract and by the prime contractor or next higher-tier subcontractor for the subcontract or supplier agreement. The CMMC level determination is made in accordance with 32 CFR 170.19, CMMC scoping. CMMC includes the following CMMC Levels: CMMC Level 1 (Self); CMMC Level 2 (Self); CMMC

Level 2 (C3PAO); and CMMC Level 3 (DIBCAC). See 32 CFR 170.14, CMMC Model.

DoD did not incorporate the recommendation to limit inclusion of CMMC in existing contracts unless the risk warrants inclusion, as contracting officers already have the discretion to bilaterally incorporate the clause in existing contracts based on DoD's needs. The determination to modify existing contracts after the effective date of this rule is up to the contracting officer consistent with other contractual requirements.

Comment: A respondent recommended that a clause fill-in with the CMMC level required by the program office should be added.

Response: Based on the public comment, a CMMC level fill-in has been added to the clause.

Comment: A respondent recommended that the rule should be reworded to require continued compliance with the CMMC level required by the contract for assets in scope for the applicable CMMC level.

Response: The rule stipulates that continued compliance with the requirements of 32 CFR part 170 is necessary for the life of the contract when there is a CMMC requirement in the contract.

Comment: A few respondents recommended that the rule be updated to clarify for FCI only, CMMC Level 1 is required.

Response: This recommendation was not included in the final rule. Contracting officers do not determine the required CMMC level, and the DFARS is written for the contracting workforce.

5. COTS Item Exclusion

Comment: A few respondents requested clarification on the awards to which the proposed rule's COTS item exclusion applies. Another respondent requested clarification on whether awards exclusively for COTS items include awards to entities that sell generally in the commercial marketplace. A respondent asked for clarification on the definition of COTS items and whether it is limited to items that individual companies have sold or applies to products that are generally sold in the commercial marketplace. A respondent stated that it is unclear if the intent of the clause exclusion applies to only COTS items. Another respondent recommended deleting the exclusions in favor of a CyberAB certification capability with no cost access to companies as a function of CyberAB SPRS certificate reporting.

Response: As described in this preamble, this 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. Any awards that are exclusively for items that meet the FAR definition would be considered "exclusively COTS" awards. CMMC assessments are conducted on contractor-owned information systems to ascertain compliance with the designated FAR, DFARS, and National Institute of Standards and Technology (NIST) requirements.

6. Extending the Certification Time for New Bidders

Comment: A respondent requested an extension of the certification time for new bidders. The respondent recommended

award timing expectations should be clearly marked in request for proposals/request for quotations documentation to ensure newer contractors are prepared to complete their certification in time for that contract award, allowing for self-evaluation for new contractors with financial impact/incentive for failure/completion of the final certification within a set time period or extending award time to allow new Defense Industrial Base members bidding on a contract to complete certification based on their response to the request for quotations.

Response: In accordance with the CMMC program policy codified at 32 CFR part 170, there is a requirement for contractors to have a CMMC self-assessment or CMMC certification, if required by the contract, at the time of award. The CMMC program policy at 32 CFR part 170 does not provide for delayed implementation for new bidders; however, 32 CFR 170.21 allows for a POA&M in certain instances.

7. Flowdown Requirements when Subcontractors Use Prime Contractor Information System

Comment: A few respondents requested clarification on whether subcontractors that use prime contractors' information systems, but not their own, would have a flowdown of CMMC requirements and whether the CMMC requirement will be the same as the prime contractor. Another respondent recommended that a requirement should be added to the clause to require that primes know the score each subcontractor has entered into SPRS, ensure the CMMC certification is current, ensure they retain copies of

affirmation statements the subcontractors provide to DoD as part of the subcontractors' CMMC compliance program, and take timely actions to remediate or mitigate the security threats to FCI and CUI caused by subcontractors that are unable to gain and maintain CMMC certification.

Response: A subcontractor that does not process, store, or transmit FCI or CUI on its subcontractor information systems during performance of the subcontract would not have a requirement for a CMMC assessment. While DoD does not have an automated tool that provides upper-tier suppliers with visibility into certification status and allows the prime to access information contained in SPRS, subcontractors may voluntarily share their CMMC SPRS assessment scores or certificates in order to facilitate business teaming arrangements.

8. Definitions

a. CUI

Comment: A respondent recommended defining CUI in the rule. Another respondent stated that "CUI" needs clarification as it relates to operational versus technical. Several respondents stated that the definition of CUI should be streamlined to match the definition of "covered defense information" in the clause at DFARS 252.204-7012, 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 that needs safeguarding as DoD "Controlled

Unclassified Information" using the same definition in the proposed rule.

Response: The definition of CUI included in the rule incorporates the definition that was codified at 32 CFR part 170. Modifying the definition of CUI beyond the codified definition at 32 CFR part 170 is outside of the scope of this rule.

b. FCI

Comment: A respondent requested clarification of the definition of Federal contract information and requested it clarify what is meant by "not intended for public release" and "simple transactional information." The respondent also asked for clarification of whether information that could be subject to a Freedom of Information Act request is still FCI and requested that the rule mark FCI.

Response: Based on public comments, a definition of FCI was added to the rule. The definition is based on the definition of FCI in the clause at FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems. This rule does not define "not intended for public release" as that is already in plain language. The definition of FCI provides "information necessary to process payments" as an example of "simple transactional information." Any comments related to marking information or Freedom of Information Act requirements are outside of the scope of this rule.

c. Current

Comment: A respondent stated that it is unclear whether the term "current" refers to current as of the date of assessment or date of certification. One respondent (#65) stated that "current" in the rule should be further defined as "no material changes in CMMC compliance since the date of the assessment".

Response: The final rule changes the definition of "current" to address these questions. The requirements for what is considered "current" under this rule were established in 32 CFR part 170. This DFARS rule implements the contractual requirements of 32 CFR part 170. Therefore, DoD cannot make the recommended change in this rule.

d. Data

Comment: Several respondents asked for clarification on the use of the term "data" and recommended the Government narrowly define the categories of data to which the rule applies (e.g., CUI or FCI). Another respondent recommended replacing "data" with a defined term, such as "FCI or CUI", to limit the scope of the requirement. Several respondents stated that the rule is unclear regarding data that is not FCI or CUI. A respondent stated the proposed requirement for contractors to only process, store, or transmit data on information systems with an appropriate CMMC certification fails to specify if data refers specifically to CUI/FCI regulated by CMMC, potentially expanding coverage to contractor data that does not include CUI or FCI.

These respondents mentioned that added clarity is necessary to ensure small business construction firms can compete for DoD

procurements. Another respondent stated that confusion related to handling of "data" on different systems can be clarified by stating the contractor "will maintain CMMC Level 1 (Self) on all systems that store, process, or transmit FCI for this contract, and will maintain Conditional or Final CMMC Level 2 (Self) / 2 (C3PAO) / 3 (DIBCAC) on all systems that store, process, or transmit CUI for this contract."

A few respondents recommended changing the sentence at DFARS 252.204-7021 paragraph (b)(3) to refer to FCI and/or CUI in lieu of "data" in the sentence to narrow the scope. A few other respondents requested clarification of the term "data" and whether that includes FCI and CUI. Another respondent asked whether CMMC is required when CUI is present but it is not DoD CUI.

Response: Based on public comments, the rule has been revised to remove the term "data." The rule applies to information that is FCI and CUI only.

e. Contractor information systems

Comment: A respondent stated that the term "contractor information systems" should be limited to the scope of "covered contractor information systems", as it appears to extend the scope of applicability to systems unrelated to CUI and FCI. Another respondent stated that the Title 32 CFR proposed rule covered, "any information system associated with the contract efforts that process, store, or transmit FCI or CUI, and to any information system that provides security protections for such

systems; or information systems not logically or physically isolated from all such systems", which is different from the scope of the Title 48 proposed rule. Another respondent recommended the Government narrowly define what the term "contractor information system" means or revert to the old term "covered contractor information system."

Response: The use of contractor information system throughout the rule includes words that follow it to clarify that the rule applies only to contractor information systems "that process, store, or transmit FCI or CUI in performance of the contract."

9. Regulatory Impact Analysis Estimate

Comment: Several respondents recommended the Regulatory Impact Analysis (RIA) be updated. A couple of the respondents recommended using all offerors in the RIA estimate based on the assumption of the cost to the industrial base to certify in anticipation of award. A respondent stated that the phased roll-out does not reduce financial impact on small businesses and recommended deleting this language from the RIA. The respondent stated the RIA estimate is too low given the time to familiarize with 889 pages of instructions. The respondent recommended including awards for FCI in the RIA estimate. The respondent also stated that the RIA underestimates the costs for assessments.

A respondent stated that the RIA cost estimate is low. The respondent further stated there are studies, data, and estimates for cost of implementing ISO 9001, and the CMMC audit process

for many companies will be on the order of half of the cost of for a company, who did not yet have a certified ISO 9001 system, implementing and achieving ISO 9001 certification. The respondent also stated the cost could put companies out of business.

A respondent asked how the Government determined that "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." The respondent stated program offices have increased the amount of data being marked as FCI or CUI, and this average of 5 contractor information systems does not reflect the DIB.

Response: The RIA associated with this rule only includes a cost analysis of the contractual requirements to upload self-assessments and complete affirmations in SPRS. The rule for the CMMC program that was codified at 32 CFR part 170 contains the expected cost impact and benefits of technical requirements associated with the CMMC program. Any comments on the cost estimates of technical or programmatic requirements related to the CMMC program affecting 32 CFR part 170 are outside of the scope of this rule.

Based on the comments, the RIA has been revised to expand the number of estimated impacted entities to include in years four and beyond all entities in the Federal Procurement Data System awarded DoD contracts from fiscal year (FY) 2022 to FY 2024. It

is unknown how many entities will be awarded contracts with a requirement to process, store, or handle FCI, CUI, or both on contractor information systems. That data then was decreased by an assumed factor to exclude entities for exclusively COTS item awards, given the number of exclusively COTS item awards is not tracked. The estimate of five information systems per contractor, on average, is a DoD subject matter expert estimate, as DoD does not have data on the number of information systems that process, store, or handle FUI, CUI, or both.

10. Application to Fundamental Research

Comment: A respondent stated that the expectation to apply CMMC to fundamental research if the fundamental research has the potential to become CUI is unreasonable and the phrase should be deleted. Another respondent stated that having a publicly available, comprehensive framework that catalogs and explains the bases for identifying edge cases in relation to the department's established policy on fundamental research is vital. The respondent requested a series of examples or scenarios in which it can see the potential for a fundamental research project to face CMMC requirements. Another respondent stated that application to fundamental research needs to be carefully considered. A few respondents recommend the applicability to fundamental research and architect and engineering services should be considered and carefully implemented.

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 once the data becomes CUI. Additionally, other research-related information that is provided to or handled by contractors as part of contract performance may be FCI or CUI, and thus may trigger application of the CMMC requirements.

11. Applicability

Comment: A couple of respondents recommended that the following language be added to the rule at DFARS 204.7502, paragraph (a) and at 204.7503, paragraph (b)(1)(i): "Systems processing FCI and not CUI require a CMMC Level 1 self-assessment" to allow a contractor that only does some DoD work to continue to use its existing and compliant business systems for the processing of FCI and build an enclave at the higher security requirement level for CUI.

Another respondent recommended the program manager document the rationale for the CMMC level required in the solicitation provision to avoid "default" CMMC level decisions. Another respondent stated that after each CMMC level, the words "(Self)" or "(C3PAO)" or "(DIBCAC)" should be added at DFARS 204.7503(i). Another respondent stated that it is unclear whether a

subcontract at or below the micro-purchase threshold would have a requirement for CMMC.

A respondent stated that it appears the review does not apply to existing contracts, only new contracts, and asked how much time there is to be compliant if a contract is modified to include the requirement for CMMC. Another respondent asked for clarification as to whether there will be modifications to existing contracts to add CMMC to the contracts. A couple of respondents stated that DFARS 252.204-7021 paragraph (b)(3) of 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 respondents recommended deleting this requirement because it is too broad and instead relying on DFARS 252.204-7012. A respondent further recommended that the Government should require coordination between the contracting officer and the contractor on how to mark subcontract information.

A respondent stated that contracting officers should not have to validate CMMC compliance prior to extending a period of performance and that this should be deleted from the rule. Another respondent asked for clarification on whether CMMC is required when partnering with an organization based on a memorandum of understanding or other data sharing arrangement that is not a "contract." The respondent asked what happens if a vendor is required to get a quote from a supplier based on a CUI drawing. The respondent asked whether companies selling

original equipment manufacturer products (e.g., Dell, Microsoft) need to achieve CMMC certification. Another respondent asked whether cyber-consulting services for contractors and subcontractors would be required to comply. A respondent asked whether spot checks could be used for CMMC instead of applying it broadly. Several respondents asked which information systems CMMC applies to. Several respondents asked whether a CMMC level could be achieved post-award instead of at the time of award.

Response: The clause will be included in solicitations issued on or after the effective date of the final rule and in any resulting contracts. The contracting officer may decide 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 also have the discretion to bilaterally incorporate the clause in contracts awarded prior to the effective date of the clause, with appropriate consideration. See FAR 1.108(d).

Until three years after the effective date of the rule, a requirement for CMMC will be present if program managers and requiring activities make a determination to apply a CMMC requirement to contracts, excluding awards solely for the acquisition of COTS items. After that, a requirement for CMMC will be present if program managers and requiring activities determine that the contractor will be required to use contractor information systems that process, store, or transmit FCI or CUI.

As described in this 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. The CMMC program codified at 32 CFR part 170 does not allow for spot checks. The requirements at 32 CFR part 170 establish that the CMMC requirement must be met at the time of award.

12. Flowdown

Comment: A respondent requested a clarification on why CMMC is flowed down to all subcontractors, but the requirement only applies when the CMMC certification requirements must be flowed down to subcontractors at all tiers when the subcontractor will process, store, or transmit FCI or CUI. Another respondent stated that the rule should add instructions to clarify that not all subcontractors must be forced to receive CUI that explicitly states a CDRL should not include or be considered CUI or that states a prime is only able to provide non-CUI portions to their FCI subcontractors. Another respondent requested clarification for how contractors and subcontractors are managed in SPRS.

A respondent stated that there needs to be a process for determining the appropriate CMMC Assessment Level for lower tiers of the supply chain based on the type of information flowed down to suppliers. Several respondents stated that there should be more guidance related to subcontractor flowdown. A few respondents stated that prime contractors do not always know what information would be flowed down to subcontractors and recommended a statement on flowdown that Level 2 is not required

when there is not a present need for the subcontractor to handle CUI, and that the subcontractor should default to Level 1 until such time as Level 2 may be required.

Response: See 32 CFR 170.23, CMMC application to subcontractors, for guidance on CMMC flowdown. The language in this rule at paragraph (d)(1) of the clause has been revised to clarify that flowdown is only required when there is a requirement under the subcontract or other contractual instrument for a CMMC level, because the subcontract or other contractual instrument will contain a requirement to process, store, or transmit FCI or CUI in performance of the subcontract or other contractual instrument. The rule has been revised at paragraph (d)(1) to no longer exclude from flowdown to subcontractors paragraph (b)(3) of the clause at 252.204-7021, which requires contractors to complete the affirmation of continuous compliance. The rule has not been revised to clarify that not all subcontractors must receive CUI or that a prime contractor is only able to provide non-CUI portions to their FCI subcontractors, as it is up to the prime contractor to determine the information that needs to be shared with a subcontractor.

13. CMMC as an Evaluation Factor

Comment: A respondent asked if CMMC was a competition evaluation factor or set-aside requirement.

Response: CMMC is not an evaluation factor or set-aside requirement. DFARS 204.7503 requires that contracting officers shall not award a contract, task order, or delivery order to an

offeror that does not meet the CMMC requirements identified in the solicitation. If CMMC is included in a solicitation, it is also included as a contract requirement.

14. Program Office Requirements

Comment: One respondent recommended adding language to the rule to require the program office to review information provided by the contractor.

Response: Based on the public comment, the rule has been revised to include language to ensure the contracting officer works with the program office or requiring activity to review the information related to the offeror's CMMC status and affirmation.

15. Clarifying when FCI Applies

Comment: A few respondents recommended making clear that information systems processing FCI but not CUI only need CMMC level 1.

Response: This recommendation was not included in the final rule. The DFARS is written for the contracting workforce. Contracting officers do not determine the required CMMC level.

16. International Applicability

Comment: A respondent stated that they are concerned the C3PAO community will not be able to perform assessments outside of the United States. Another respondent recommended DoD continue its outreach to global partners and allies to promote international harmonization and mutual recognition of required assessments and regulations. Another respondent asked whether

the approval of the certification or the verification of the self-assessment results be determined by the United States, or whether an authorized Taiwanese verification body, such as TAF, can issue the certification. The respondent also asked whether compatibility with Taiwanese law should be considered and if long-term jurisdiction applies. The respondent questioned the corresponding upstream cybersecurity architecture that supports this framework, i.e., the blueprint for the cybersecurity architecture of this supply chain. Another respondent requested that DoD clarify whether it might deem relevant international cybersecurity standards or frameworks as equivalent to CMMC and, if so, what timeline and process would govern such determination.

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. Any contract that is subject to the existing requirements to comply with NIST SP 800-171 (e.g., via DFARS 252.204-7012) would require the contractor, whether foreign or domestic, to secure their information systems. CMMC assessment requirements serve to validate current security compliance requirements. Respondents with interest in international or non-US based C3PAOs should review 32 CFR 179, which does not preclude otherwise qualified foreign companies from achieving C3PAO accreditation. Note that DoD permits C3PAO personnel who are not eligible to obtain a

Tier 3 background investigation to meet the equivalent of a favorably adjudicated Tier 3 background investigation. DoD will determine the Tier 3 background investigation equivalence for use with the CMMC Program only.

17. POA&M

Comment: A respondent recommended adding language related to POA&Ms closeout in the final rule. Another respondent stated that pursuant to 32 CFR part 170.21, POA&Ms are permissible if certain conditions are met and recommended the rule mention a conditional certification as a viable option for subcontract award. The respondent also recommended amending DFARS 204.7501 to clarify that conditional certifications are acceptable for subcontract award if the conditions in 32 CFR part 170.21 are met. Another respondent stated that 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. The rationale is that POA&Ms are part of the NIST SP 800-171 framework, so contractors should have the latitude to continue to adopt POA&Ms without being considered by DoD to have fallen out of "continuous compliance." Another respondent recommended the final rule allow 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.

Response: Based on the public comments, the rule has been revised to clarify, by amending the definition of "current", that for CMMC levels 2 and 3 only, a conditional CMMC status is permitted for a period not to exceed 180 days from the conditional CMMC status. DoD also amended the solicitation provision and contract clause to clarify that a final CMMC status is achieved upon successful closeout of a POA&M. The CMMC program policy codified at 32 CFR part 170 establishes the guidelines related to POA&Ms and does not allow for additional POA&Ms outside of the established scoping in 32 CFR part 170, other than for scenarios that are appropriate for an operational plan of action, as defined in 32 CFR 170.4.

18. Subcontractor Compliance

Comment: Several respondents asked for clarification on how prime contractors are expected to monitor and verify CMMC adherence of subcontractors. A respondent stated that since SPRS access is limited for prime contractors to validate supplier compliance, there is no way of confirming eligibility. Another respondent requested clarification on whether subcontractors will need to provide a screenshot of CMMC compliance. Several respondents recommended creating an automated tool that provides upper-tier suppliers with visibility into certification status without revealing supporting artifacts or that the rule limit the scope of DFARS 252.204-7021 paragraph (b)(6) to direct suppliers, without requiring enforcement throughout the entire supply chain. A

respondent stated that SPRS should adopt a function to forward SPRS statuses upon request by a subcontractor cryptographically or should be updated to allow voluntary sharing of subcontractor's records with higher tier contractors. A couple of respondents stated that prime contractors should access a baseline of information on subcontractors in SPRS to reduce reporting burden. A few other respondents recommended that SPRS allow DIB companies to query the database to validate subcontractor compliance with CMMC requirements.

Response: Contractors will only be able to access their own CMMC certificate or CMMC self-assessment information. DoD does not have a tool 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 for any other clause requirement that flows down to subcontractors. The prime contractor's responsibility is to flow down CMMC assessment requirements as described in 32 CFR 170.23 and to not disseminate FCI or CUI to subcontractors that have not indicated they meet the CMMC level described in 32 CFR 170.23 for the type of information to be shared. Likewise, subcontractors must also flow down CMMC requirements or not disseminate FCI or CUI to suppliers that have not indicated they meet the CMMC level required, as described in 32 CFR 170.23, for the type of information to be shared.

There is not an automated process to allow prime contractors to view the CMMC status of subcontractors. SPRS will allow subcontractors to print or take a screen shot of their own CMMC status and affirmation information in SPRS, which they can share as they determine appropriate. In addition, subcontractors will be able to provide copies of their CMMC certification for level 2 (C3PAO) and CMMC level 3 (DIBCAC) status.

The CMMC policy codified at 32 CFR 170 does not provide for limiting the scope of the rule to direct suppliers without requiring enforcement throughout the entire supply chain.

Comment: Several respondents recommended the final rule clarify at what point subcontractors must be compliant and allow enough time for primes to conduct subcontractor due diligence and for the prime contractor to "decompose" the CMMC level required down the supply chain. A respondent recommended the final rule specify that a prime contractor ensure its subcontractors have the appropriate CMMC level prior to awarding a subcontract or other contractual instrument.

Response: The rule states that prior to awarding a subcontract or other contractual instrument, the prime contractor shall ensure that the subcontractor has a current CMMC status at the CMMC level that is appropriate for the information to be flowed down.

Comment: A few respondents recommended updating SPRS to improve reporting functionality during the phase-in period to reduce requirements to report to the contracting officer

manually and to allow for automated updates to CMMC information for prime contractors.

Response: The determination of which CMMC UIDs are applicable to a particular contract are determined by the contractor. As a result, there is not a way to automatically update the contracting officer with the applicable CMMC UIDs for a particular solicitation or contract.

Comment: A couple of respondents stated that the exclusion of paragraphs (b)(5) and (c) in the clause at DFARS 252.204-7021 appear to be in conflict with how prime contractors manage updates in SPRS. The respondents stated that it was unclear whether the CMMC exception at the subcontract level was only for subcontracts exclusively for COTS items. They also stated that it was unclear how primes manage subcontractor compliance.

Response: This rule clarifies in the clause that the CMMC requirements for entering self-assessments into SPRS, not covered by a C3PAO assessment or DIBCAC assessment, flow down to subcontractors in addition to the requirement to complete the affirmation of continuous compliance.

19. Senior Company Official

Comment: A respondent stated that the term "senior company official" cannot be found anywhere in the 32 CFR proposed rule which instead refers to an "affirming official", described in section 170.22 as "the OSA senior official who is responsible for ensuring OSA compliance with CMMC Program requirements." The respondent also stated it is unclear whether the affirmation

is expected for each contract or at the information system UID level.

Another respondent stated that the term "senior company official" is unclear because it is unclear what "senior" means, which could cause compliance issues. A respondent recommended in lieu of the "senior company official" DoD use the term "senior accountable official for risk management" from the NIST Computer Security Resource Center, which is defined as "the senior official, designated by the head of each agency, who has vision into all areas of the organization and is responsible for alignment of information security management processes with strategic, operational, and budgetary planning processes."

A few respondents stated that "senior company official" should be removed from the rule so that contractors can designate an appropriate official within their organization to make the affirmation of continuous compliance and noted that the requirement at DFARS 252.204-7019 does not require a "senior company official." A respondent stated that absent the inclusion of a regulatory and legal safe harbor for contractors in the rulemaking, DoD should remove the reference to a senior company official from the proposal and that the wording around a senior company official is undefined and vague in its applicability to contractors and subcontractors. Another respondent encouraged DoD to provide a clear definition of "senior company official" in the final rule.

Response: The proposed rule used the term that was included in the proposed rule affecting 32 CFR part 170, because the intent was to use consistent terms. However, as part of the public comment period adjudication, the 32 CFR part 170 rule updated the term to "affirming official." Based on timing, the proposed DFARS rule was published with the old term. The terminology has been modified in this final rule to align with the term "affirming official" that was codified at 32 CFR part 170.

20. Task Orders and Delivery Orders

Comment: One respondent requested clarification on whether existing indefinite-delivery indefinite-quantity contracts that have task orders or delivery orders after publication of the final DFARS rule will contain a CMMC requirement.

Response: The rule prescribes use of the solicitation provision at DFARS 252.204-7025 and the contract clause at DFARS 252.204-7021 in certain solicitations and contracts, task orders, or delivery orders. Therefore, task orders or delivery orders issued after this rule takes effect may include a requirement for CMMC.

21. Relationship Between the Terms "Covered Contractor Information Systems" and "Contractor Information Systems"

Comment: Several respondents asked for clarification on the relationship between the term "covered contractor information systems" from the clause at DFARS 252.204-7012 and "contractor information systems" from the clause at DFARS 252.204-7021. A

respondent stated that use of "contractor information systems" will broaden the scope of applicability to information systems which, because they are not "covered", are unrelated to CUI and FCI.

Another respondent stated that the scope of what constitutes an "information system" should be defined by contractors following the approach used by the Cybersecurity and Infrastructure Security Agency in the common form for Secure Software Development Framework-related attestations. Another respondent recommended expressly permitting contractors to define the scope of the "information system" that applies to a given CMMC UID requirement and also cited the approach used by the Cybersecurity & Infrastructure Security Agency. A respondent recommended specifying more clearly the scope of an information system that is associated with the CMMC UID requirements. Another respondent recommended adding a definition of "contractor information system" to the rule and defining that term to mean "an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information, CUI, or FCI. It does not include commercial communications networks that transmit government and nongovernment information using the same equipment, protocols, and methodologies, without regard to the source or recipient of the information."

Response: The rule includes language that clarifies that contractor information systems that are impacted by the rule are

contractor information systems that process, store, or transmit FCI or CUI during performance of the contract.

22. CMMC Unique Identifiers

Comment: Several respondents requested clarification on DoD UIDs, which are now referred to as "CMMC UIDs". A respondent asked for clarification on the relationship between the term "DoD Unique Identifier" and Commercial and Government Entity (CAGE) codes and asked for clarification regarding how contractors may define "contractor information system" for purposes of generating CMMC UIDs for systems that process, store, or transmit only FCI. A few respondents recommended either continuing to use the CAGE code linkages in SPRS used today for tracking compliance to DFARS 252.204-7020 or clarifying how the CMMC UID process will work and be used. A respondent asked for clarification on how an information system is identified in relation to CMMC UIDs. A respondent stated that the rule should make it clear that CMMC UIDs are mandatory throughout, as in one place it appears mandatory and in the other it appears to be required at the request of the contracting officer. Several respondents stated DoD should clarify in its rulemaking whether contractors must provide CMMC UIDs only for a contractor's own information systems or also for their subcontractors' information systems that will process, store, or transmit FCI or CUI during performance of the contract.

Response: In accordance with the requirements established at 32 CFR part 170, it is not possible to provide additional clarification in this rule regarding information systems associated with the UID, because the UID is assigned for the CMMC Assessment Scope as defined by the Organization Seeking Assessment (OSA). Specifically, 32 CFR 170.19 (Scoping) explains that a CMMC assessment is conducted against a specific scope of assets in the environment of the OSA. The scope of assets is the information system or systems or components that will be assessed against CMMC security requirements and is defined by the OSA.

In the process of submitting the results of a CMMC assessment, SPRS or the Enterprise Mission Assurance Support Service (eMASS) system assigns a UID to be associated with that assessment scope and reflected in SPRS. OSAs must identify in their offers to solicitations each UID that describes the scope (i.e., assets, systems, components) that will be used to process, store, or transmit FCI or CUI for a given contract, so DoD can check SPRS to verify that the appropriate CMMC assessment requirement has been met. As specified in 32 CFR 170.15 and 32 CFR 170.16, SPRS inputs include the industry CAGE codes(s) associated with the information system(s) addressed by the CMMC Assessment Scope. OSAs will need a CAGE code and an account in SPRS to complete the annual affirmation required for all CMMC assessments. To do so, OSAs should obtain a CAGE code via *https://sam.gov* before registering in the Procurement Integrated Enterprise Environment

(PIEE). Businesses outside of the United States must obtain a NATO Commercial and Government Entity (NCAGE) code from *https://eportal.nspa.nato.int/Codification/CageTool/home*. Instructions for obtaining a PIEE account can be found on the PIEE Vendor Account website: *https://piee.eb.mil/xhtml/unauth/web/homepage/vendorGettingStartedHelp.xhtml*.

The rule clarifies that only prime contractors with a CMMC requirement will be required to submit CMMC UIDs to the contracting officer for any contractor information system that will process, store, or transmit FCI or CUI during performance of the contract, which may include the CMMC UIDs associated with the contractor information systems of the prime's subcontractors. Subcontractors do not have a requirement to submit CMMC UIDs to the contracting officer. As with any subcontract requirement, the prime will need to work with the subcontractor to obtain the subcontractor's CMMC UIDs, if applicable.

Comment: A respondent recommended that DoD adopt the language proposed in DFARS 204.7503 paragraph (b)(2) that requires the contractor to provide the CMMC UID for each system the contractor is utilizing for contract performance that houses the relevant information.

Response: The rule clarifies that contractors are required to submit to the contracting officer CMMC UID(s) issued by SPRS or eMASS for the contractor information systems that process,

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

Comment: A respondent asked for clarification on whether a company will have one UID or if it will have a UID for each contractor information system.

Response: A CMMC UID will be issued for each assessment required for a system or systems identified by the offeror as being used to process, store, or transmit FCI or CUI during performance of the contract.

Comment: A respondent expressed that the public should be aware that a new UID is generated for each SPRS score entered for that system, and the original UID will be replaced when there is a new score entered at 3 years or if a significant change necessitates a reassessment.

Response: When results of a CMMC assessment are submitted in SPRS, SPRS assigns a CMMC UID to be associated with that assessment scope. Thus, if the results of a new assessment are submitted, SPRS will reflect a new CMMC UID to be associated with that assessment scope.

23. Creation of Exception

Comment: A respondent stated that DoD should consider providing for relief from CMMC demands in exceptional circumstances, so that the regulation does not prove disadvantageous to the programs, systems, and capabilities that it is intended to protect. Another respondent stated that small business entities should be exempted from CMMC Level 2

requirements when they are second-tier suppliers and not receiving information flowed to the prime. A respondent also recommended that DoD delay inclusion of CMMC in existing contracts since the supply chain for the contract already exists.

Response: The CMMC rule codified at 32 CFR part 170 established the requirements for CMMC and does not include an exemption for exceptional circumstances. Thus, this DFARS rule is unable to make that change.

DoD does not require the flowdown of CMMC requirements to subcontractors that do not receive FCI or CUI from the prime contractor.

The determination related to the CMMC implementation plan timeline was made in 32 CFR 170. This DFARS rule is unable to change the CMMC Program rule.

24. Period of Performance

Comment: A respondent stated that contracting officers should not have to validate CMMC compliance prior to extending a period of performance and that this should be deleted from the rule. Another respondent stated that the rule should adopt language proposed in DFARS 204.7503 paragraph (b)(2) that requires the contractors provide this information to DoD; specifically, the DoD unique identifier (now CMMC UID) for each system the contractor is utilizing for contract performance that houses the relevant information.

Response: The CMMC program policy codified at 32 CFR part 170 requires CMMC statuses to be maintained for the life of the contract. Therefore, contracting officers must validate CMMC compliance prior to extending the period of performance or exercising an option in accordance with the codified policy at 32 CFR part 170. This rule includes the requirement for the contractor to provide the required CMMC UIDs to the contracting officer to allow for verification of the information in SPRS.

25. Prime Contractor Protection from Subcontractor Noncompliance

Comment: A respondent stated that the rule should clarify that prime contractors will not be rendered ineligible for award if DoD concludes that a subcontractor does not have a timely or sufficient certification status in SPRS and that the prime should be alerted by the contracting officer regarding subcontractor noncompliance. Another respondent stated that the rule should clarify the relationship, roles, and responsibilities between the prime and subcontractor.

Response: The Government does not establish the relationship between the prime contractor and its subcontractors, nor does it indemnify the prime contractor from its subcontractors. This is because the Government does not have privity of contract with subcontractors.

26. Application of CMMC to FAR Part 16 Contract Types

Comment: Several respondents stated that the rule should be updated to require approval by the CMMC Program Office and or

the Office of the Under Secretary of Defense for Acquisition and Sustainment before including a requirement for CMMC in solicitations and contracts that use FAR part 16 contract types prior to the end of the phased in roll-out.

Response: The CMMC rule codified at 32 CFR part 170 established the requirements for the application of CMMC and does not include an approval process. Thus, this rule is unable to make that change.

27. Acquiring Entities without CMMC Certification

Comment: A respondent asked if a new entity is acquired or DoD work will otherwise be supported at a site not initially included in the entity's CMMC certification, whether there will be a mechanism to add the new entity or site to the existing certification. The respondent also asked if the new entity or site will use the same information technology systems and follow the same policies and procedures, whether the entity or site could be deemed covered under an existing certification.

Response: In accordance with DFARS 252.204-7021 paragraph (c)(1), contractors are required to report to contracting officers any changes to the list of UIDs that process, store, or transmit FCI or CUI and that are used in performance of the contract. Adding new users to an existing system does not necessarily change the scope of a CMMC assessment. See 32 CFR 170.19, CMMC Scoping.

28. Applicability to Civilian Agencies

Comment: A respondent expressed that DoD should clarify whether CMMC applies to CUI from non-DoD agencies.

Response: The rule amends the DFARS, so this rule only includes requirements for DoD or acquisitions for which DoD funding is used.

29. Provision and Clause Clarifications

Comment: A respondent recommended the clause be updated to include a requirement to require subcontractors to provide any updates to CMMC UID data in SPRS. Another respondent asked whether the rule intended to remove paragraph (b)(5) of the clause from subcontract flowdown. Another respondent expressed that paragraph (b)(5) and (c) of the clause should be harmonized with how contractors and subcontractors are managed in SPRS. Another respondent stated there needs to be clarification on what is meant by "unless electronically posted" in SPRS with respect to the proposed language in the provision at DFARS 252.204-7YYY.

Response: As a result of the comments, the clause has been updated in this rule to clarify that subcontractors are required to enter in SPRS the results of self-assessment(s) for each CMMC UID applicable to each of their contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract. Subcontractors will have the ability to take a screen shot of their CMMC status and affirmation responses in SPRS to be able to share that information as they deem necessary. The clause has also been

updated in this rule to clarify that subcontractors are required to complete on an annual basis, and maintain as current, an affirmation of continuous compliance by the affirming official in SPRS. The requirement of paragraph (b)(3) of the clause is intended to be flowed down as described in the clause language.

The words "unless electronically posted" in SPRS are not included in this final rule. The comment related to paragraphs (b)(3) and (c) of the clause is noted. The paragraphs are harmonized between the contractor and subcontractor actions. The Government does not have privity of contract with the subcontractor, thus paragraphs(c)(1) of the clause are excluded from the subcontractor flowdown requirements. However, prime contractors should consider flowing down substantially similar language in subcontracts to help them avoid sharing FCI or CUI with subcontractors that are not compliant with requirements to safeguard such information.

30. Outside the Scope of the Rule

Comment: DoD received several comments that are outside the scope of this rule. Some of the topics addressed in the out-of-scope comments included the following: timeline for publication of DFARS Case 2022-D017, NIST SP 800-171 DoD Assessment Requirements; marking information; modifying the clause at DFARS 252.204-7012; the National Archives and Records Administration's definition of "CUI"; requirements to coordinate on CUI with the contractor; invitation to speaking engagement; and sharing of a personal web address.

Other out-of-scope comments addressed the underlying CMMC program policy codified at 32 CFR part 170, which is separate from this rule. Some of the CMMC Program-related topics included the following: permissible changes in a CMMC certified environment; exemption from CMMC requirements for Morale, Welfare, and Recreation / Nonappropriated Fund funded products, information technology commercial services, and fulfilment/delivery services; training the Government and public on CMMC; the relationship between CMMC and ISO/IEC 27001; definitions established under the final rule codified at 32 CFR part 170; early implementation of CMMC; affirmation requirements established at 32 CFR part 170; the definition of CUI codified at 32 CFR part 170; intent to require FCI handling within the CUI-certified boundary; joint technical development effort recommendations for European original equipment manufacturers; cost impact to small entities and ways to provide relief; documentation of program manager rationale for CMMC selection; guidance on CMMC level selection; CMMC Level 2 certification vs. self-assessment; security data protections; application to medical device suppliers; application to subcontractors; subcontractor compliance requirements; enclave approach; duplicative assessments; application to mobile devices; application to medical devices; guidance on how CMMC will handle updates to NIST SP 800-171; phase-in timeline; application to furniture manufacturers; relationship with common carrier systems; harmonization of CMMC across Federal agencies; number

of assessors; potential delays and unintended consequences from CMMC; evaluating Cloud Service Providers; oversight of program managers when determining a CMMC level; FedRAMP compliance; applicability to warranty, installation, or training services; FCI requirements; streamlining CMMC requirements through spot checks; billing and cost allowability; guidance on waivers; and training on eMASS.

Response: These comments are outside the scope of this DFARS rule. Regarding the CMMC level selection, the program office or requiring activity will determine the CMMC level in accordance with DoD policy and 32 CFR 170.5, Policy. The CMMC level will be identified in the solicitation provision and contract clause. Contracting officers will not make determinations related to the CMMC level. DoD has issued guidance to the program offices and requiring activities related to CMMC level selection.

Regarding whether a CMMC Level 2 certification or self-assessment would be required, in accordance with DoD policy, all categories of CUI would necessitate a self-assessment. In general, CUI categories from the DoD Organizational Index group would necessitate a C3PAO assessment, at a minimum.

Regarding Morale, Welfare and Recreation / Nonappropriated Fund procurements, if those procurements include a requirement to provide basic safeguarding of FCI or CUI through implementation of NIST SP 800-171, then the CMMC requirement should also apply.

Waiver requirements were established at 32 CFR 170.5. It should be noted that waivers are at the discretion of the program office or requiring activity and are determined prior to the contracting officer's involvement in the procurement.

Regarding eMASS, contractors do not have access to CMMC eMASS, as that system is used to support certification assessments only. All CMMC assessments are reflected in SPRS.

This DFARS rule cannot update requirements related to determining cost allowability as those requirements are located at FAR 31.201-2.

The affirmation requirements were codified at 32 CFR 170.22. This DFARS rule reflects the requirements established at 32 CFR part 170.

Regarding FCI handling within the CUI-certified boundary, the intent of CMMC is not to require all FCI handling to occur within the CUI-certified boundary.

With regard to the enclave approach, the contractor determines the systems(s) that will be used in performance of a DoD contract and the assessment scope that must be specified in advance of an assessment at any CMMC level, as detailed in 32 CFR part 170.19.

Regarding the phased implementation plan, the implementation requirements for the phase-in of CMMC were codified at 32 CFR part 170.3.

With regard to reassessments, the final rule affecting 32 CFR part 170 was modified to clarify that reassessments may be

required based on post-assessment indicators of cybersecurity issues or noncompliance and are different from new assessments that occur when an assessment validity period expires. Reassessment is expected to be infrequent and conducted by DoD.

Flowdown requirements are established at 32 CFR 170.23, Application to Subcontractors. Guidance for determining the CMMC level is addressed in DoD policy (*https://dodprocurementtoolbox.com/uploads/DOPSR_Cleared_OSD_Memo_CMMC_Implementation_Policy_d26075de0f.pdf*) and at 32 CFR 170.5. Subcontractors are to comply in the same way as the prime contractor, with the exception of sharing CMMC UID data with the contracting officer.

Regarding cyber incidents and CUI, the requirements of CMMC, which is an assessment framework, are separate from the cyber incident reporting requirements in the clause at DFARS 252.204-7012. Therefore, cyber incident reporting comments are unrelated to CMMC. This DFARS rule is unrelated to the CUI program. As such, comments related to CUI and CUI designations are outside of the scope of this rule.

C. Other Changes

Other minor changes were made in the final rule. The final rule was updated at DFARS 204.7500 to remove a web address and replace it with a reference to 32 CFR part 170, now that the CMMC program requirements have been codified at 32 CFR part 170. A clarification has been made throughout to indicate that a

higher CMMC level than required will also be permissible under the rule.

The text has been updated throughout the rule to include the term "CMMC status." This terminology was established in 32 CFR part 170 and clarifies that contracts may be awarded if there is a current Final Level 1 (Self), Conditional Level 2 (Self), Final Level 2 (Self), Conditional Level 2 (C3PAO), or Final Level 2 (C3PAO) CMMC status. In addition, the definition of "CMMC status" has been added to the rule in DFARS subpart 204.75, the contract clause at 252.204-7021, and the solicitation provision at 252.204-7025.

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

The clause at DFARS 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements, is prescribed at DFARS 204.7504 for use, until three years after the effective date of the rule, in solicitations and contracts, task orders, or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, except for those solely for the acquisition of commercially available off-the-shelf (COTS) items, if the program office or requiring activity determines that the contractor is required to have a specific CMMC level, unless the requirements at 32 CFR 170.5(d) are met.

On or after three years and one day after the effective date of the rule, the clause is prescribed for use in solicitations and contracts, task orders, or delivery orders, 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 COTS items, if the program office or requiring activity determines that the contractor is required to use contractor information systems in the performance of the contract, task order, or delivery order to process, store, or transmit FCI or CUI. The provision at DFARS 252.204-7025, Notice of Cybersecurity Maturity Model Certification Level Requirements, is prescribed at DFARS 204.7504(b) for use in solicitations that include the clause at DFARS 252.204-7021.

Consistent with the analysis that DoD provided in the proposed rule with regard to the application of the requirements of section 1648 of the NDAA for FY 2020, DoD has made the determination to apply the statute, as implemented in the clause at DFARS 252.204-7021 and the provision at DFARS 252.204-7025, to contracts at or below the SAT, for the acquisition of commercial products, excluding COTS items, and to the acquisition of commercial services, as defined at FAR 2.101.

IV. Expected Impact of the Rule

A. Background

DoD is amending the DFARS to implement the contractual requirements related to the DoD policy for CMMC (see the final

rule codifying 32 CFR part 170, published in the **Federal Register** October 15, 2024, at 89 FR 83092). CMMC self-assessments and third-party assessments assess a contractor's compliance with certain information system security requirements. Pursuant to the DoD CMMC policy at 32 CFR part 170, the CMMC level requirements apply to contractor information systems that will process, store, or transmit FCI or CUI.

DoD is amending the DFARS to include the following solicitation and contractual requirements related to the CMMC policy:

- Offeror and contractor requirement to post the results of a CMMC Level 1 or Level 2 self-assessment to 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 status for the life of the contract.
- Contractor requirement for an affirming official (see 32 CFR 170.4) to complete an affirmation of continuous compliance with the security requirements identified at 32 CFR part 170 in SPRS for each CMMC 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 compliance status changes occur.
- 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 CMMC UIDs generated by SPRS.

The costs associated with the technical completion of the CMMC third-party assessments and self-assessments are included in the CMMC final rule affecting title 32 CFR.

B. Summary of Impact

This final 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 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 implementation plan, 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.

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 those 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, task orders, or delivery orders solely for the acquisition of COTS items.

Using data from the Federal Procurement Data System for the calculations for the fourth year and beyond, the average number of unique entities for FY 2022 through FY 2024 who received awards above the micro-purchase threshold is 32,756. This number includes 18,370 unique awardees who were awarded contracts using only commercial procedures. DoD does not track awardees and awards exclusively for COTS items. Therefore, it is assumed that of the 18,370 entities who were awarded contracts using only commercial procedures, 25%, or 4,592, were awarded contracts exclusively for COTS items. To remove COTS-only awardees from the total, DoD subtracted 4,592 from the 32,756 unique entities with contracts above the micro-purchase threshold, which results in 28,164 unique entities.

DoD does not track the number of unique offerors per award, so DoD assumes 2 offerors per solicitation on average. To account for offerors for prime contracts, DoD multiplied 28,164 by 2, which is 56,328 offerors. DoD does not track subcontractors, because it does not have privity of contract with subcontractors. Therefore, it is assumed that for every prime contractor offer, there are 5 subcontractors included in the

proposal. As a result, the total number of impacted entities is estimated to be 337,968 unique entities, which includes prime contractors and subcontractors. Of those unique entities, 229,818 (68%) are estimated to be small entities.

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 CMMC UIDs in SPRS for the information systems that will be used in performance of the contract and to submit the CMMC UIDs to the Government.

DoD assumes it will take the Government—

- An estimated 5 minutes to validate the existence in SPRS of the correct CMMC level and currency of a CMMC status associated with offeror CMMC UIDs for all offerors 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 in SPRS of the correct level and currency of a CMMC status and

affirmation associated with contractor CMMC UIDs, when there are changes in the information systems during contract performance.

The primary cost impact of this final rule is that offerors and contractors 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 252.204-7025, Notice of Cybersecurity Maturity Model Certification Level Requirements, and the clause at DFARS 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements.

The benefits of this final rule include verification of a defense industrial base (DIB) contractor's implementation of system security requirements that must be applied by all Federal agencies for the protection of FCI and CUI. The clause at DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, implements Federal safeguarding requirements but does not provide for DoD verification of a DIB contractor's implementation of the security requirements specified in NIST SP 800-171 prior to contract award. CMMC adds the element of verification of a DIB contractor's cybersecurity through the use of certified third-party assessors. This 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 flowdown to its subcontractors in a multi-tier supply chain.

Another benefit of this final 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. 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 10-year period, that burden would equate to an estimated $400 billion to $765 billion in costs at a 7 percent discount rate and an estimated $486 billion to $929 billion in costs at a 3 percent discount rate. In addition, the Government Accountability Office (GAO) has reported the economic impacts of ransomware as being devastating to the nation's security, and cited Department of Treasury reports that "the total value of U.S. ransomware-related incidents reached $886M in 2021."

The following is a summary of the estimated public and Government costs calculated over a 10-year period at a 3 percent discount rate:

SUMMARY	Public	Government	Total
Present Value	$329,097,922	$15,812,069	$344,909,991
Annualized Costs	$38,580,316	$1,760,303	$40,340,619

The following is a summary of the estimated public and Government costs calculated over a 10-year period at a 7 percent discount rate:

SUMMARY	Public	Government	Total
Present Value	$254,756,766	$11,533,649	$266,290,415
Annualized Costs	$36,271,632	$1,642,132	$37,913,764

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. Executive Order 14192

The rule is not subject to the requirements of E.O. 14192, because this rule is being issued with respect to a national security function of the United States. Implementation of the CMMC Program requirements in contracts is urgently needed to strengthen protection of DoD information. Our Nation cannot afford to continue development of DoD's critical mission capabilities without securing them against cyber-attacks. The primary benefit of the CMMC Program requirements is securing contractor information systems against adversaries seeking to exfiltrate the Government's information related to some of the

Nation's most valuable, advanced defense technologies. Additionally, the contractual requirements of the CMMC Program will help the DIB protect its own intellectual property from exfiltration, which will protect the U.S. economy from billions of dollars of damage inflicted by malicious cyber actors.

Application of the requirements of E.O. 14192 to this rule would unacceptably impede DoD's ability to implement the contractual requirements associated with a verification mechanism to ensure the DIB maintains a current and effective cybersecurity posture as a condition of contract award. Without this rule, DoD's ability to maintain technological advantages and secure our warfighting programs will be jeopardized, which will put U.S. critical infrastructure at risk of failure or disruption. This increased risk affects all intellectual property and sensitive DoD information held by defense contractors and can leave industry susceptible to devastating financial losses. For these reasons, DoD finds the implementation of the contractual requirements of the CMMC Program critical to national security.

VII. Congressional Review Act

As required by the Congressional Review Act (5 U.S.C. 801-808) before an interim or final rule takes effect, DoD will submit a copy of the interim or final rule with the form, Submission of Federal Rules Under the Congressional Review Act, to the U.S. Senate, the U.S. House of Representatives, and the Comptroller General of the United States. A major rule under the

Congressional Review Act cannot take effect until 60 days after it is published in the **Federal Register**. The Office of Information and Regulatory Affairs has determined that this rule is not a major rule as defined by 5 U.S.C. 804(2).

VIII. Regulatory Flexibility Act

A final regulatory flexibility analysis has been prepared consistent with the Regulatory Flexibility Act, 5 U.S.C. 601, *et seq*. and is summarized as follows:

This final 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 as well as DoD controlled unclassified information. This final rule includes the following requirements for all offerors responding to a solicitation, and contractors awarded contracts, containing a requirement for Cybersecurity Maturity Model Certification (CMMC):

(1) Post in the Supplier Performance Risk System (SPRS) the results of a current CMMC status for each CMMC unique identifier (CMMC UID), not covered by a CMMC third-party assessment organization (C3PAO) assessment or Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) assessment at the CMMC level required by the solicitation, or higher, for CMMC UIDs applicable to each of the contractor information systems that will process, store, or transmit Federal contract information

(FCI) or controlled unclassified information (CUI) and that will be used in performance of the contract;

(2) Maintain the CMMC status at the required CMMC level for the life of the contract;

(3) Provide the CMMC UID(s) applicable to each of those contractor information systems to the contracting officer and provide updates, if applicable; and

(4) Have a current affirmation of continuous compliance with the security requirements identified at 32 CFR part 170 in SPRS for each CMMC UID applicable to each of those contractor information systems.

These requirements apply to offerors responding to solicitations containing a CMMC requirement and to contractors with a CMMC requirement in contracts prior to exercising an option.

These requirements do not apply to awards that do not involve the handling or transmission of FCI or CUI.

The final 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 CMMC 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 National Defense Authorization Act for Fiscal Year (FY) 2020. Specifically, this rule implements paragraph (c)(2) of section 1648.

The public did not submit comments in response to the initial regulatory flexibility analysis. However, DoD received public comments regarding the costs associated with the CMMC program itself, which is outside of the scope of this rule. Those costs have been addressed in the final rule affecting 32 CFR part 170.

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. 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.

During the phased implementation period, the estimated number of small entities to which the rule will apply is 1,104 in year one, 5,565 in year two, and 18,554 in year three. By the fourth year, all offerors responding to solicitations for DoD contracts and orders who have contractor information systems that will be used in performance of the contract or order to process, store, or transmit FCI or CUI will be required to have a minimum of a CMMC Level 1 self-assessment or the CMMC level identified in the

solicitation and resulting contract, task order, or delivery order, or higher, except for contracts or orders exclusively for COTS items. The program office or requiring activity will determine the CMMC level that is appropriate for the type of information to be handled under the contract.

By year four, and beyond, the estimated number of impacted small entities will be 229,818, which includes prime contractors and subcontractors that are small entities. DoD has no way to track contractors awarded contracts or orders exclusively for COTS items, offerors responding to DoD solicitations exclusively for COTS items, or offerors for subcontracts exclusively for COTS items. Therefore, these values are estimated based on input by subject matter experts.

Using data from the Federal Procurement Data System, the average number of unique entities for FY 2022 through FY 2024 who received awards above the micro-purchase threshold is 32,756. This number includes 18,370 unique entities who were awarded contracts using only commercial procedures. DoD does not track awardees and awards exclusively for COTS items. Therefore, DoD assumed that of the 18,370 entities who were awarded contracts using only commercial procedures, 25%, or 4,592, were awarded contracts exclusively for COTS items. To remove COTS-only awardees from the total, DoD subtracted 4,592 from the 32,756 unique entities with contracts above the micro-purchase threshold, which results in 28,164 unique entities.

DoD does not track the number of unique offerors per award, so

DoD assumed 2 offerors per solicitation on average. To account for offerors for prime contracts, DoD multiplied 28,164 by 2, which is 56,328 offerors. DoD does not track subcontractors, so it is assumed based on expertise that for every prime contractor offer, there are 5 subcontractors included in the proposal. The 56,328 offerors are multiplied by a factor of 6 (i.e., 1 prime offeror plus 5 subcontractors) to account for the assumed number of subcontractors included in offers for prime contracts. As a result, the total number of impacted entities is estimated to be 337,968 unique entities, which includes prime contractors and subcontractors. Of those unique entities, 229,818 (68%) are estimated to be small entities.

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 status is required and, if so, at what CMMC level:

CMMC Level	Percentages	Small Entities	Large Entities	Total Entities
Level 1 Self-assessment	62%	142,487	67,053	209,540
Level 2 Self-assessment	2%	4,596	2,163	6,759
Level 2 Certificate	35%	80,436	37,853	118,289
Level 3 Certificate	1%	2,298	1,082	3,380
Total Entities	100%	229,818	108,150	337,968

This final 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 final rule:

(1) A requirement for offerors to post results of a current CMMC status, not covered by a C3PAO or DIBCAC assessment, to SPRS for each CMMC UID applicable to each of the contractor information systems that will be used in performance of the contract to process, store, or transmit FCI or CUI;

(2) A requirement for offerors to provide CMMC UIDs for each of those contractor information systems, if applicable, prior to award and when any changes to CMMC UIDs occur; and

(3) A requirement for an affirming official (see 32 CFR 170.4) 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 CMMC UID applicable to each of those contractor information systems.

These reporting requirements would apply to any small entities that are offerors responding to a solicitation that includes 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 status of Level 1 (Self) or Level 2 (Self). The requirement to provide CMMC UIDs and the requirement for the affirming official to complete the affirmation in SPRS will apply to all small entities that are

offerors for a solicitation or contractors awarded a contract that includes a requirement for CMMC.

There are no known alternatives that would accomplish the stated objectives of the applicable statute. This final rule uses a phased rollout approach to implementation and applies the CMMC requirements only to offerors for solicitations and contractors awarded a contract containing a CMMC requirement until three years after the effective date of the rule. On or after three years and one day after the effective date of the rule, the CMMC requirements apply only to solicitations and contracts when the contractor will be required to use contractor information systems in the performance of the contract, task order, or delivery order to process, store, or transmit FCI or CUI.

This final rule exempts contracts and orders exclusively for the acquisition of COTS items to minimize any significant economic impact of the final 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 final rule.

IX. Paperwork Reduction Act

This final rule contains information collection requirements that have been approved by the Office of Management and Budget under the Paperwork Reduction Act (44 U.S.C. chapter 35). This information collection requirement has been assigned OMB Control

Number 0750-0008, Defense Federal Acquisition Regulation Supplement (DFARS) Part 204, Contractor Implementation of Cybersecurity Requirements.

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

Government procurement.

Kimberly R. Ziegler,

Editor/Publisher, Defense Acquisition Regulations System.

Accordingly, the interim rule amending 48 CFR parts 204, 212, 217, and 252, which was published at 85 FR 61505 on September 29, 2020, is adopted as final with the following changes:

1. The authority citation for 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.

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 information security protections.

(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.

(c) This subpart applies to unclassified contractor information systems.

204.7501 Definitions.

As used in this subpart—

Controlled unclassified information means information the Government creates or possesses, or information 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—

(1) With regard to Conditional Cybersecurity Maturity Model Certification (CMMC) Status—

(i) Not older than 180 days for Conditional Level 2 (Self) assessments and Conditional Level 2 (certified third-party assessment organization (C3PAO)) assessments, with—

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Conditional CMMC Status date (see 32 CFR 170.16 and 170.17); and

(B) A corresponding affirmation of continuous compliance by an affirming official (see 32 CFR 170.4); and

(ii) Not older than 180 days for Conditional Level 3 (Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)) assessments, with—

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Conditional CMMC Status date (see 32 CFR 170.18); and

(B) A corresponding affirmation of continuous compliance by an affirming official;

(2) With regard to Final CMMC Status—

(i) Not older than 1 year for Final Level 1 (Self), with—

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Final CMMC Status date (see 32 CFR 170.15); and

(B) A corresponding affirmation of continuous compliance, not older than 1 year, by an affirming official;

(ii) Not older than 3 years for Final Level 2 (Self) assessments and Final Level 2 (C3PAO) assessments, with—

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Final CMMC Status date (see 32 CFR 170.16 and 170.17); and

(B) A corresponding affirmation of continuous compliance, not older than 1 year, by an affirming official; and

(iii) Not older than 3 years for Final Level 3 (DIBCAC) assessments, with—

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Final CMMC Status date (see 32 CFR 170.18); and

(B) A corresponding affirmation of continuous compliance, not older than 1 year, by an affirming official; and

(3) With regard to affirmation of continuous compliance (32 CFR 170.22), not older than 1 year with no changes in compliance with the requirements at 32 CFR part 170.

Cybersecurity Maturity Model Certification (CMMC) status means the result of meeting or exceeding the minimum required score for the corresponding assessment. The potential statuses are as follows:

(1) Final Level 1 (Self).

(2) Conditional Level 2 (Self).

(3) Final Level 2 (Self).

(4) Conditional Level 2 (C3PAO).

(5) Final Level 2 (C3PAO).

(6) Conditional Level 3 (DIBCAC).

(7) Final Level 3 (DIBCAC).

Cybersecurity Maturity Model Certification unique identifier (CMMC UID) means 10 alpha-numeric characters assigned to each

CMMC assessment and reflected in the Supplier Performance Risk System (SPRS) for each contractor information system.

Federal contract information (FCI) means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government. It does not include information provided by the Government to the public, such as on public websites, or simple transactional information, such as information necessary to process payments.

204.7502 Policy.

(a) *Award eligibility*. (1) The contracting officer shall include in the solicitation the required CMMC level, if provided by the program office or the requiring activity.

(2) Contracting officers shall not award a contract, task order, or delivery order to an offeror that does not have a current CMMC status at the CMMC level required by the solicitation.

(3) Contractors are required to achieve, at time of award, a CMMC status at the CMMC level specified in the solicitation, or higher, for all information systems used in the performance of the contract, task order, or delivery order that will process, store, or transmit FCI or CUI. Contractors are required to maintain a current CMMC status at the specified CMMC level or higher, if required by the contract, task order, or delivery order, throughout the life of the contract, task order, or delivery order.

(b) *CMMC status*. (1) Contracting officers may award a contract, task order, delivery order, or modification to exercise an option or extend a period of performance, if the offeror's or contractor's CMMC status is—

(i) Listed in the definition of "CMMC status"; and

(ii) Equal to or higher than the CMMC level required by the solicitation or contract, task order, or delivery order.

(2) CMMC levels 2 and 3 can be in a conditional level for a period not to exceed 180 days from the CMMC status date (32 CFR 170.21), and award can occur with a conditional CMMC level. CMMC level 1 requires a final CMMC level for award.

204.7503 Procedures.

(a) *CMMC level*. The contracting officer shall include the CMMC level (see 32 CFR 170.19) required by the program office or requiring activity in the solicitation provision and contract clause prescribed at 204.7504.

(b) *Award*. Contracting officers shall check SPRS and not award a contract, task order, or delivery order to an offeror that does not have a current CMMC status posted in SPRS at the CMMC level (see 32 CFR 170.15 through 170.18) required by the solicitation, or higher, for each CMMC UID provided by the offeror. The CMMC UIDs are 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.

(c) *Option exercise or period of performance extension*. Contracting officers shall check SPRS and not exercise an option

or extend the period of performance on a contract, task order, or delivery order, unless the contractor has a current CMMC status posted in SPRS at the CMMC level (see 32 CFR 170.15 through 170.18) required by the contract, task order, or delivery order, or higher, for each CMMC UID provided by the contractor. The contractor's CMMC UIDs are applicable to each of the contractor information systems that process, store, or transmit FCI or CUI and that are or will be used in performance of the contract.

(d) *CMMC UIDs*. If the contractor provides new CMMC UIDs during performance of the contract, task order, or delivery order, the contracting officer shall check in SPRS, using the CMMC UIDs assigned by SPRS, that the contractor has a current CMMC status at the required CMMC level, or higher, for each of the contractor information systems identified that will process, store, or transmit FCI or CUI during contract performance.

204.7504 Solicitation provision and contract clause.

(a) Unless the requirements at 32 CFR 170.5(d) are met, use the clause at 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements, as follows:

(1) Until November 9, 2028, in solicitations and contracts, task orders, or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, except for those solely for the acquisition of commercially available off-the-shelf (COTS) items, if the

program office or requiring activity determines that the contractor is required to have a specific CMMC level.

(2) On or after November 10, 2028, in solicitations and contracts, task orders, or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, except for those solely for the acquisition of COTS items, if the program office or requiring activity determines that the contractor is required to use contractor information systems in the performance of the contract, task order, or delivery order to process, store, or transmit FCI or CUI.

(b) Use the provision at 252.204-7025, 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 by—

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

b. 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 252.204-7025, Notice of Cybersecurity Maturity Model Certification Level Requirements, as prescribed in 204.7504(b).

* * * * *

PART 217—SPECIAL CONTRACTING METHODS

4. Revise section 217.207 to read as follows:

217.207 Exercise of options.

(c) In addition to the requirements at FAR 17.207(c), exercise an option only after—

(1) Determining that the contractor's record in the System for Award Management database is active and the contractor's unique entity identifier number, Commercial and Government Entity (CAGE) code, name, and physical address are accurately reflected in the contract document. See PGI 217.207 for the requirement to perform cost or price analysis of spare parts prior to exercising any option for firm-fixed-price contracts containing spare parts; and

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

(i) The summary level score of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old, unless a lesser time is specified in the solicitation) for each covered contractor information system that is relevant to an offer, contract, task order, or delivery order are posted (see 204.7303); and

(ii) If there is a requirement for the contractor to have a Cybersecurity Maturity Model Certification (CMMC) status at a specific CMMC level, the contractor has a current CMMC status at the CMMC level required by the contract, or higher, for each of the CMMC unique identifiers applicable to each of the contractor information systems that process, store, or transmit Federal contract information or controlled unclassified information (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), use the following clause:

CONTRACTOR COMPLIANCE WITH THE CYBERSECURITY MATURITY MODEL CERTIFICATION LEVEL REQUIREMENTS (NOV 2025)

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

Controlled unclassified information means information the Government creates or possesses, or information 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—

(1) With regard to Conditional Cybersecurity Maturity Model Certification (CMMC) Status—

(i) Not older than 180 days for Conditional Level 2 (Self) assessments and Conditional Level 2 (certified third-party assessment organization (C3PAO)) assessments, with—

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Conditional CMMC Status date (see 32 CFR 170.16 and 170.17); and

(B) A corresponding affirmation of continuous compliance by an affirming official (see 32 CFR 170.4); and

(ii) Not older than 180 days for Conditional Level 3 (Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)) assessments, with—

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Conditional CMMC Status date (see 32 CFR 170.18); and

(B) A corresponding affirmation of continuous compliance by an affirming official;

(2) With regard to Final CMMC Status—

(i) Not older than 1 year for Final Level 1 (Self), with—

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Final CMMC Status date (see 32 CFR 170.15); and

(B) A corresponding affirmation of continuous compliance, not older than 1 year, by an affirming official;

(ii) Not older than 3 years for Final Level 2 (Self) assessments and Final Level 2 (C3PAO) assessments, with—

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Final CMMC Status date (see 32 CFR 170.16 and 170.17); and

(B) A corresponding affirmation of continuous compliance, not older than 1 year, by an affirming official; and

(iii) Not older than 3 years for Final Level 3 (DIBCAC) assessments, with—

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Final CMMC Status date (see 32 CFR 170.18); and

(B) A corresponding affirmation of continuous compliance, not older than 1 year, by an affirming official; and

(3) With regard to affirmation of continuous compliance (32 CFR 170.22), not older than 1 year with no changes in compliance with the requirements at 32 CFR part 170.

Cybersecurity Maturity Model Certification (CMMC) status means the result of meeting or exceeding the minimum required score for the corresponding assessment. The potential statuses are as follows:

(1) Final Level 1 (Self).

(2) Conditional Level 2 (Self).

(3) Final Level 2 (Self).

(4) Conditional Level 2 (C3PAO).

(5) Final Level 2 (C3PAO).

(6) Conditional Level 3 (DIBCAC).

(7) Final Level 3 (DIBCAC).

Cybersecurity Maturity Model Certification unique identifier (CMMC UID) means 10 alpha-numeric characters assigned to each CMMC assessment and reflected in the Supplier Performance Risk System (SPRS) for each contractor information system.

Federal contract information (FCI) means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government. It does not include information provided by the Government to the public, such as on public websites, or simple transactional information, such as information necessary to process payments.

Plan of action and milestones means a document that identifies tasks to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones, as defined in National Institute of Standards and Technology Special Publication 800-115 (32 CFR 170.21).

(b) *Framework*. The Cybersecurity Maturity Model Certification (CMMC) is a framework for assessing a contractor's compliance with applicable information security protections (see 32 CFR part 170).

(c) *Duplication*. 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.

(d) *Requirements.* The Contractor shall—

(1)(i) Have and maintain for the duration of the contract a current CMMC status at the following CMMC level, or higher: _____ *[Contracting Officer insert: CMMC Level 1 (Self); CMMC Level 2 (Self); CMMC Level 2 (C3PAO); or CMMC Level 3 (DIBCAC)]* for all information systems used in performance of the contract, task order, or delivery order that process, store, or transmit FCI or CUI; and

(ii) Consult 32 CFR 170.23 related to the flowdown of the CMMC requirements, and flow down the correct CMMC level to subcontracts and other contractual instruments;

(2) Only process, store, or transmit FCI or CUI on contractor information systems that have a CMMC status at the CMMC level required in paragraph (d)(1) of this clause, or higher;

(3) Complete on an annual basis, and maintain as current, an affirmation, by the affirming official (see 32 CFR 170.4), of continuous compliance with the requirements associated with the CMMC level required in paragraph (d)(1) of this clause in the Supplier Performance Risk System (SPRS) (*https://piee.eb.mil*) for each CMMC 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;

(4) Ensure all subcontractors and suppliers complete prior to subcontract award, and maintain on an annual basis, an affirmation, by the affirming official (see 32 CFR 170.4), of

continuous compliance with the requirements associated with the CMMC level required for the subcontract or other contractual instrument for each of the subcontractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the subcontract; and

(5) If the Contractor has a CMMC Status of Conditional, successfully close out a valid plan of action and milestones (32 CFR 170.21) to achieve a CMMC Status of Final.

(e) *Reporting*. The Contractor shall—

(1) Submit to the Contracting Officer—

(i) The CMMC UID(s) issued by SPRS for contractor information systems that will process, store, or transmit FCI or CUI during performance of the contract; and

(ii) Any changes in the CMMC UIDs generated in SPRS throughout the life of the contract, task order, or delivery order, if applicable;

(2) Enter into SPRS the results of a current self-assessment for each CMMC UID, not covered by a C3PAO assessment or DIBCAC assessment, 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) Complete in SPRS on an annual basis and maintain as current an affirmation of continuous compliance by the affirming official (see 32 CFR 170.4) for each self-assessment, C3PAO assessment, or DIBCAC assessment required under the contract in SPRS.

(f) *Subcontracts.* The Contractor shall—

(1) Insert the substance of this clause, including this paragraph (f) and excluding paragraph (e)(1), in subcontracts and other contractual instruments, including those for the acquisition of commercial products and commercial services, excluding commercially available off-the-shelf items, if the subcontract or other contractual instrument will contain a requirement to process, store, or transmit FCI or CUI; and

(2) Prior to awarding a subcontract or other contractual instrument, ensure that the subcontractor has a current CMMC certificate or current CMMC status at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor based on the requirements at 32 CFR 170.23.

(End of clause)

6. Add section 252.204-7025 to subpart 252.2 to read as follows:

252.204-7025 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 (NOV 2025)

(a) *Definitions.* As used in this provision, *controlled unclassified information (CUI)*, *current*, *Cybersecurity Maturity Model Certification (CMMC) status*, *Cybersecurity Maturity Model Certification unique identifier (CMMC UID)*, *Federal contract information (FCI)*, and *Plan of action and milestones* 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 level required by this solicitation is: _____ *[Contracting Officer insert: CMMC Level 1 (Self); CMMC Level 2 (Self); CMMC Level 2 (C3PAO); or CMMC Level 3 (DIBCAC)]*. This CMMC level, or higher (see 32 CFR part 170), 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 Offeror will not be eligible for award of a contract, task order, or delivery order resulting from this solicitation if the Offeror does not have, 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—

(i) The current CMMC status 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

(ii) A current affirmation of continuous compliance with the security requirements identified at 32 CFR part 170 in SPRS.

(c) *Plan of action and milestones*. If the Offeror has a CMMC Status of Conditional, the Offeror shall successfully close out

a valid plan of action and milestones (32 CFR 170.21) to achieve a CMMC Status of Final.

(d) *CMMC unique identifiers*. The Offeror shall provide, in the proposal, the CMMC unique identifier(s) (CMMC UIDs) 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 Offeror also shall update the list when new CMMC UIDs are generated in SPRS. The CMMC UIDs are provided in SPRS after the Offeror enters the results of self-assessment(s) for each such information system.

(End of provision)

[FR Doc. 2025-17359 Filed: 9/9/2025 8:45 am; Publication Date: 9/10/2025]